MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Service du commissariat des armées

CONCOURS EXTERNE SUR ÉPREUVES
DE RECRUTEMENT D'ÉLÈVES COMMISSAIRES DES ARMÉES EN 2021

ÉPREUVE DE NOTE DE SYNTHÈSE

durée : 4 heures – coefficient 7

Vous êtes affecté(e) à la Direction générale du numérique et des systèmes d'information et de communication (DGNUM) du ministère des armées.

En vue de son audition prochaine par la commission de la défense nationale et des forces armées de l'Assemblée nationale portant sur la stratégie du ministère en matière numérique, le directeur général vous demande de lui préparer, à partir du dossier joint, une note faisant le bilan des avancées nationales en matière de cybersouveraineté, sur lesquelles se fonderont des propositions d'actions pour le ministère des armées dans ce domaine d'ici à cinq ans.

Ce travail de synthèse ne doit pas dépasser 900 mots, avec une marge de tolérance de plus ou moins dix pour cent, soit entre 810 et 990 mots.

Cybersouveraineté

SOMMAIRE

How ‘Cybersovereignty’ Splits the Once World Wide Web

By Karen Leigh, Stepan Kravchenko, and Saritha Rai
May 2nd 2019

Early on, the narrative around the internet was it should be unfettered and borderless, a global commons. That didn’t last. China’s President Xi Jinping has led the way in asserting what’s become known as cybersovereignty -- a nation’s right to control the digital realm. Other authoritarian regimes such as Russia’s and Vietnam’s, but also governments in places such as India and France, are following suit. With America’s more hands-off approach under fire for enabling election meddling, fake news and hate speech, China is trumpeting its method of controlling the internet to serve state interests.

1. What’s cybersovereignty?

Being sovereign means having the power to set the rules. Applied to cyberspace, it means a government controlling how the internet is used within its borders and what happens with the data generated. China coined the term and imposed what’s known as the Great Firewall, which censors online discourse and can scrub sensitive historic events -- like the 1989 Tiananmen massacre in Beijing -- from online records. The government also limits which news sites, search engines, shopping portals and social-media platforms are available to users and what apps can be downloaded. Under a 2017 law, China also requires electronic data be stored in-country and be accessible on demand to the authorities.

2. How is it enforced?

To get online, consumers in China are restricted to using state-owned carriers, which must toe the party line. Websites like Facebook and Google are banned outright. China began blocking Facebook’s WhatsApp encrypted messaging service, used by over 1 billion people around the world, in 2017. (Homegrown rival WeChat, owned by Tencent Holdings Ltd., is unencrypted.) Online gaming is restricted. The government reviews new titles to vet content; video game approvals were frozen for months in 2018, hammering the shares of gaming companies. Even the #MeToo movement fell victim, with the Communist Party taking measures to stop a growing wave of accusations of sexual misconduct being circulated online.

3. Who else is doing it?

Some recent examples:

- Russian lawmakers passed a “sovereign internet” bill allowing authorities to manage internet traffic nationwide and, if needed, cut it off from the outside world. The new legislation also could make it easier for Moscow to stifle communication during times of civil unrest or disrupt encrypted messaging apps. Russia already censors a variety of topics online and blocks foreign companies like LinkedIn and Zello that don’t locate servers inside the country.

- India's central bank requires payment firms like Mastercard and Visa to store data exclusively on local servers, a rule that could be expanded under a broader e-commerce policy being considered.
- In Southeast Asia, home to more than half a billion people whose internet economy is expected to triple to $240 billion by 2025, autocratic regimes in Vietnam and Thailand are passing laws mirroring China's model of content curbs and data controls.
- The French National Assembly formed a task force in April 2018 to examine ways to protect against not only cyberattacks but growing dependency on foreign technology companies, after a French Senate report warned France and the European Union were at risk of becoming "digital colonies."
- Freedom House's 2018 report on digital authoritarianism noted that China, which it called the worst abuser of internet freedom, hosted representatives from 36 countries at training sessions on handling new media or information management.

4. Is cybersovereignty about security or censorship?

Cybersovereignty enables both censorship -- the suppression of information for political or other purposes -- and cybersecurity, the protection of things like transportation systems, electrical grids and personal information. Xi, who chairs China's top cyber-administrative regulator, has repeatedly underscored the importance of building an independent cyberspace that foreign powers can't disrupt, as the foundation for China's national security. President Vladimir Putin described Russia's new legislation as a response to the threat of surveillance by the U.S. National Security Agency.

5. Why is the data vital?

Today's digital world generates far more information about individuals than ever before, so-called "big data" that can be parsed, analyzed and then exploited. Companies use the data to target advertising, hone their products or develop "deep learning" algorithms. The Chinese government uses such data to keep tabs on its citizenry -- companies are required to hand it over if requested. Thailand's new law grants the government the right to seize data and electronic equipment without a court order in the interests of national security. India has made concerted efforts to safeguard its own digital assets, including legislative measures to keep information and data from flowing out from the country, partly to help domestic startups.

6. Are there ways around cyber controls?

Virtual private networks, known as VPNs, can be used to circumvent internet restrictions. Beijing has clamped down on VPNs, which exist in a legal gray area, but they are widely used elsewhere. Greatfire.org, a non-profit group that opposes censorship, has created mirrored sites and a browser to get around China's restrictions. Telegram Messenger LLP dodges attempts by authorities in Moscow to block its use in Russia by constantly changing IP addresses. Even many Kremlin officials are still using the messaging app.

7. Where is this headed?

Ex-Google Chief Executive Officer Eric Schmidt has predicted that within a decade, the internet will split in two, with one led by the U.S. and the other by China. A big test will be the global expansion of Chinese tech titans such as Tencent and Alibaba Group Holding Ltd., which developed and flourished within China's authoritarian model.

Cyberdéfense : quelle stratégie pour la France ?

Claire Landais
Secrétaire générale de la défense et de la sécurité nationale *

Contestation des fonctions régaliennes, attaques informatiques, protection des câbles sous-marins, ... une politique de souveraineté numérique doit impérativement prendre en compte la cyberdéfense. Tour d'horizon de la stratégie de la France présenté par Claire Landais, Secrétaire générale du Secrétariat général de la défense et de la sécurité nationale (SGDSN) lors de son audition devant la commission d'enquête du Sénat sur la Souveraineté numérique

[...] « Pour avoir une vision globale d'ensemble sur notre souveraineté numérique, nous avons besoin de connaissances techniques pointues de certains secteurs, les personnes qui m'accompagnent aujourd'hui en témoignent. Je vous propose de vous livrer notre vision des grands enjeux de la souveraineté numérique et de répondre à toutes vos interrogations sur la manière dont le Secrétariat général de la défense et de la sécurité nationale (SGDSN), acteur de coordination, intervient sur cette problématique.

La souveraineté numérique – c'est-à-dire notre capacité à rester maître de nos choix, de nos décisions et de nos valeurs dans une société numérisée – recouvre trois aspects complémentaires.

Première composante, la souveraineté à l'ère numérique : comment préserver les composantes traditionnelles de notre souveraineté, dans un contexte où le numérique remet en question les monopoles régaliens, parce qu'il crée des acteurs de substitution ou parce qu'il fragilise les outils

*** Extrait de l'audition de Claire Landais par la commission d'enquête sur la souveraineté numérique : voir rapport n° 7 (2019-2020) de Gérard Longuet, fait au nom de la commission d'enquête du Sénat sur la Souveraineté numérique, déposé le 1er octobre 2019, «*Le devoir de souveraineté numérique – Tome II : comptes rendus*» : http://www.senat.fr/rap/r19-007-2/r19-007-21.pdf. Les intertitres et exergues ont été ajoutés par la rédaction des *Cahiers français*.**

des activités monopolistiques régaliennes ? Deuxième dimension, la souveraineté dans l'espace numérique : comment conserver notre capacité autonome d'appréciation, de décision et d'action dans le cyberespace ? [...] Enfin, troisième enjeu, la souveraineté des outils numériques : comment maîtriser nos réseaux, nos communications électroniques et nos données, publiques ou personnelles ? »

Préserver les fonctions régaliennes

« Comment, d'abord, préserver les composantes traditionnelles de notre souveraineté, dans un contexte où le numérique remet en question les monopoles régaliens ?

> ***Les États ne sont aujourd'hui plus, de fait, les seuls à pouvoir délivrer des titres attestant de l'identité de quelqu'un***

Les nouvelles technologies ont progressivement permis à des acteurs privés de rivaliser avec les États, en assumant des fonctions faisant historiquement et sans conteste jusqu'alors l'objet de monopoles régaliens. Cette tendance est en partie irréversible, ce qui ne signifie pas qu'il faille renoncer à en organiser les modalités. Chaque État se voit ainsi conduit à arbitrer entre les attributs de souveraineté qu'il choisit de préserver en priorité, et ceux qu'il peut accepter de déléguer à la sphère privée, le cas échéant de façon encadrée.

Service du Premier ministre créé en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique
© HAMILTON/REA

Je n'évoquerai pas devant vous l'attribut régalien, pourtant historiquement important, que constituent le privilège de battre monnaie ni sa remise en cause par les crypto-monnaies, du type Bitcoin, car nous dépasserions de beaucoup le champ de compétence du SGDSN.

Parmi ces grands monopoles régaliens aujourd'hui contestés, citons d'abord l'identification officielle, le privilège d'authentifier les personnes. Les États ne sont aujourd'hui plus, de fait, les seuls à pouvoir délivrer des titres attestant de l'identité de quelqu'un : de grands acteurs privés comme les réseaux sociaux, au premier rang desquels Facebook – avec Facebook Connect – jouent dorénavant le rôle de fournisseurs d'identité. Les services d'authentification qu'ils proposent sont déjà largement utilisés, à ce stade par des sites internet privés et pour des utilisations non sensibles. Le risque est réel que, sans réponse des États, de telles solutions puissent, à moyen terme, devenir de fait les identités numériques d'usage, évinçant le rôle des pouvoirs public.

L'Europe et la France ont apporté d'ores et déjà certaines réponses : la loi du 7 octobre 2016 pour une République numérique prévoit ainsi

Les administratio les entrepris ou les opérat d'importance vitale (énerg transports, santé, etc.) s victimes cha jour en Franc de plusieurs milliers d'att informatique

© [VALERYBROZ ADOBE STOCK

d'encadrer la fourniture d'identité numérique par le secteur privé, une identité numérique étant présumée fiable uniquement si elle répond à un cahier des charges établi par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Sont également développés, d'une part, un service d'authentification national – la plateforme FranceConnect conçue par la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) -, et d'autre part une identité numérique souveraine – via le projet ALICEM (Authentification en ligne certifiée sur mobile) du ministère de l'Intérieur -, en cours d'évaluation par l'ANSSI. Enfin, au niveau européen, a été introduit un cadre juridique commun, avec le règlement adopté en 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit « eIDAS », qui prévoit la reconnaissance entre les États membres et l'interopérabilité des méthodes nationales d'identifications numériques.

Autre monopole régalien par excellence, celui de la violence légitime : attaquer et défendre. Face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement étatsuniens, remettent en cause le monopole des États dans l'usage de la violence légitime. Se fondant sur une interprétation discutable du droit à la légitime défense dans l'espace cyber, qui n'est pas la nôtre, ils font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (« hack back ») qui va au-delà de la simple protection de leurs propres systèmes d'information, autorisant par exemple des intrusions dans les systèmes adverses pour les détruire. Les risques que voit la France à une telle légalisation de pratiques dans certains pays et à leur diffusion au niveau international sont bien réels : risque d'erreur d'attribution, d'abord, car face à la difficulté pour obtenir

une identification fiable de l'origine de l'attaque – et à ce titre, une action de riposte non encadrée pourrait prendre pour cible un tiers innocent ; risque de dommage collatéral et de riposte incontrôlée, d'autre part, de nature à aggraver l'instabilité du cyberespace.

Dans ce contexte, la France a choisi de maintenir l'interdiction actuellement en vigueur de cette pratique en droit français et de prôner activement son interdiction au niveau international. Ainsi, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, rendu public par le ministre de l'Europe et des Affaires étrangères le 12 novembre 2018 au Forum de Paris sur la paix, et soutenu par le Président de la République à l'occasion de son discours à l'UNESCO devant le Forum sur la gouvernance de l'internet, a été l'occasion de réaffirmer le monopole étatique de la violence légitime. Cette initiative se décline aujourd'hui de façon opérationnelle dans différents *fora*, notamment à l'organisation de coopération et de développement économiques (OCDE) et à l'Organisation des nations unies (ONU.)

Dernier attribut régalien contesté : assurer la sécurité intérieure. Il s'agit là moins de lutter contre la substitution d'acteurs privés que de répondre à l'affaiblissement des outils de l'action régalienne. L'efficacité de nos services d'enquête judiciaire et de renseignement repose dorénavant sur des technologies numériques pour lesquelles les offres nationale et européenne sont lacunaires, ce qui nous conduit à dépendre d'offres étrangères, par exemple pour le traitement de données massives et l'acquisition de capacités vulnérabilités informatiques. Il est donc essentiel que l'État travaille de concert avec l'industrie pour faire émerger des solutions nationales ou européennes. Il nous faut, en outre, pouvoir correctement faire face à l'évolution constante des normes et des outils technologiques, par exemple dans le domaine de la surveillance légale des communications pour ne pas être pris de court par le développement des réseaux 5G. »

Discours d'Emmanuel Macron lors de l'ouverture du Forum sur la gouvernance de l'internet, le 12 novembre 2018 au siège de l'UNESCO à Paris
© [POOL/REUTERS]/ ADOBE STOCK

Disposer d'une autonomie d'appréciation et de décision

« Deuxième aspect de la souveraineté numérique : Comment conserver notre capacité autonome d'appréciation, de décision et d'action dans le cyberespace ? Ce second volet de notre souveraineté numérique concerne le maintien de la capacité de l'État et, dans un certain sens, de nos entreprises et citoyens, à disposer d'une autonomie d'appréciation, de décision et d'action dans le cyberespace. »

« En ce qui concerne l'État, la France a fait le choix de conserver une autonomie de décision en matière de défense et de sécurité du cyberespace. Atteindre cet objectif repose sur une capacité souveraine à détecter les attaques informatiques qui affectent l'État et les infrastructures critiques – je pense

aux opérateurs d'importance vitale (OIV), notamment. À ce titre, l'ANSSI développe ses propres systèmes de détection pour la supervision des administrations, et ses travaux ont permis de faire émerger des solutions industrielles de confiance pour la France au profit des entreprises. L'agence a ainsi qualifié en avril 2019 les sondes de détection de deux industriels français.

En outre, nos capacités nationales de détection ont été significativement renforcées par la loi de programmation militaire pour 2019-2025. Ses dispositions permettent aux opérateurs télécoms de mettre en œuvre des dispositifs de détection au sein de leur réseau pour mieux repérer les attaques informatiques, autorisent l'ANSSI à donner à ces opérateurs des marqueurs ou signatures d'attaques informatiques pour les aider à les repérer, et ont ouvert la voie au déploiement de sondes par l'agence en cas de risque pour les systèmes informatiques de l'État, d'opérateurs d'importance vitale ou d'opérateurs de services essentiels.

Enfin la France souhaite garder une capacité souveraine à attribuer les cyberattaques. Développer et maintenir une telle capacité est un choix d'engagement majeur, qui implique de ne pas dépendre de certains de nos grands partenaires. Au vu des investissements nécessaires, la maîtrise de telles capacités ne sera accessible à terme qu'à un nombre très limité de pays qui auront fait le choix stratégique de les détenir. La France a bien l'intention d'en faire partie.

La France développe une doctrine nationale de découragement et de réaction dans le cyberespace. Elle repose sur une méthode

Antenne-rela
téléphonie m
avec mise à j
pour la 5G

nationale d'évaluation de la gravité d'une cyberattaque et un schéma de classement des cyberattaques qui intègre toute la palette des outils et normes mobilisables – et cela implique de faire se parler des acteurs de cultures parfois différentes. La réponse peut passer par la judiciarisation, se traduire par une attribution publique (« name and shame » en vue d'un impact réputationnel), voire – dans la mesure où il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée au sens de l'article 51 de la Charte des Nations Unies – par la mobilisation de capacités offensives dans le milieu cyber comme dans les autres milieux. Ce dernier point relève principalement du ministère des armées, et je renvoie au discours de Mme Florence Parly en février 2019. L'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opération extérieurs, dans le respect du droit international.

Fruit également de la revue cyber et de la réflexion sur la gouvernance, l'articulation entre dimensions défensive et offensive obéit à une doctrine qui donne la priorité à la première, tout en privilégiant le dialogue entre acteurs responsables des deux chaînes.

La France promeut, enfin, à l'international sa vision selon laquelle le droit international est applicable au cyberespace et l'attribution publique reste une décision politique qui relève de la souveraineté et ne peut donc être déléguée à une organisation internationale. Dans ce domaine, notre pays souhaite garder la main.

Pour nos entreprises, il s'agit de préserver une capacité à innover dans un contexte d'hégémonie des géants américains du numérique – mais nous sommes là sur des questions hors du champ de compétence SGDSN.

L'autonomie d'appréciation et de décision de nos citoyens passe par la préservation de la sincérité du débat démocratique, face au phénomène émergent de manipulation de l'information par des puissances étrangères. Le rôle de la société civile reste essentiel, l'État pouvant fournir des outils pour lutter contre ces manipulations, notamment en période électorale. L'Union européenne a créé un réseau d'alerte en ce sens à l'occasion des élections. »

Maîtriser nos réseaux et données

« Troisième aspect de la souveraineté numérique : Comment maîtriser nos réseaux, nos communications électroniques et nos données ? Notre souveraineté numérique passe en effet par notre capacité à protéger nos réseaux de télécommunication – et les données qui y transitent – des actions d'espionnage et de sabotage.

En matière de sécurité et de résilience des réseaux, des dispositions législatives existent déjà, dans notre code pénal notamment. Celles figurant aux articles R. 226-1 et suivants permettent un contrôle des équipements qui constituent le cœur des réseaux, pour préserver l'impératif de la protection de la vie privée et du secret des correspondances. Les demandes sont aujourd'hui instruites par l'ANSSI. Toutefois, au regard de l'importance croissante prise par les réseaux mobiles, notamment par la 5G et les nouveaux usages qu'elle permettra dans un futur bien plus proche que prévu, il paraît nécessaire d'apporter rapidement des évolutions au cadre juridique actuel, tant dans ses modalités que pour consacrer une finalité de protection de la sécurité nationale. Nous souhaiterions dès lors que puisse être soumise à autorisation préalable du Premier ministre – déléguée au SGDSN après instruction par l'ANSSI – l'exploitation de certains équipements des réseaux mobiles pour les opérateurs télécoms qui sont

En février 2018 a été publiée par le SGDSN la *Revue stratégique de cyberdéfense*, document inédit qui est présenté comme un véritable livre blanc sur la cyber défense.

opérateurs d'importance vitale. Un amendement en ce sens avait été déposé, sans suite, dans la loi « PACTE », dispositions désormais reprises par une proposition de loi en cours d'examen devant le Parlement.

La protection des réseaux passe également par celle de nos câbles sous-marins, essentiels dans l'architecture des réseaux actuels. La problématique de la résilience se double d'un enjeu d'attractivité pour notre territoire, et nos réflexions en la matière mobilisent plusieurs départements ministériels, afin que nous soyons compétitifs, notamment en termes de normes et d'interconnexions.

En matière de protection des données et des communications, les exigences sont graduées, dans une logique de cercles concentriques. Au cœur, pour les données et communications classifiées, nous devons viser une obligation de résultat, garantissant leur protection contre des attaques ciblées des adversaires les plus compétents. Cette ambition implique la maîtrise nationale de certaines technologies, au premier rang desquelles le chiffrement des communications. La France possède dans ce domaine une industrie de confiance, apte à fournir des équipements de très haut niveau de sécurité.

Pour le champ médian des données et communications sensibles, des exigences impératives doivent pouvoir être fixées, sous forme de label de l'État.

Cette déclinaison en plusieurs sphères s'applique pleinement à la question du nuage informatique (cloud). Ainsi, pour ses données stratégiques classifiées, l'État aura recours exclusivement à un cloud interne. En revanche, pour d'autres données publiques et pour les besoins des entreprises, la qualification des clouds par l'ANSSI permettra d'identifier les offres qui apportent des garanties suffisantes vis-à-vis des risques tant techniques que juridiques. Les entreprises doivent elles-mêmes faire l'effort de segmenter leurs données en fonction de leur caractère stratégique ou sensible. »

> **« Notre environnement juridique mérite également d'être adapté au rapport de force qui s'engage**

« Sur cette question du cloud, notre environnement juridique mérite également d'être adapté au rapport de force qui s'engage actuellement avec certains de nos partenaires tentés par une application extraterritoriale de leur droit. Dans la perspective de tels conflits de normes, il est essentiel pour rester crédibles de pouvoir leur opposer des outils comme le règlement général sur la protection des données (RGPD) ou une « loi de blocage » rénovée. Ces textes normatifs auront, d'une part, un effet incitatif dans les négociations qui doivent s'engager entre États et, d'autre part, un effet dissuasif sur les sociétés étrangères concernées, exposées au risque d'être en infraction avec nos normes. »

[...]

Quels moyens pour la cyberdéfense ?

« Concernant la concurrence dans le recrutement des talents, le principal obstacle reste, du point de vue de l'État, un problème de salaire. Nous souffrons souvent de la comparaison avec le privé pour conserver

nos ingénieurs et les profils industriels qui nous intéressent. Une réflexion est cependant en cours, vous le savez, sur l'évolution du droit de la fonction publique, qui devrait nous donner ces capacités de souplesse nécessaires aux recrutements dans un secteur particulièrement tendu. La DINSIC a récemment diffusé une circulaire qui rappelle la panoplie des outils de recrutement déjà utilisables. Ne négligeons pas non plus l'attrait du drapeau et la renommée de l'ANSSI, dont la réputation d'excellence permet de recruter les meilleurs éléments. Le passage par l'agence reste pour beaucoup une garantie ultérieure de reconversion ou de passerelle réussie dans le privé.

Concernant les moyens de l'ANSSI, [...] la trajectoire d'emploi est positive. Mettre des moyens dans la cyberdéfense est une priorité assumée de l'État.

La discrétion dans l'attribution des cyberattaques et la faible publicité qui leur est ainsi donnée tient d'abord, à la difficulté technique inhérente au mécanisme d'identification des responsabilités. La méthode reste celle du faisceau d'indices, et l'entraide judiciaire est compliquée, soit par mauvaise volonté, soit tout simplement par manque de compétences techniques de certains pays. Sans jamais s'interdire de donner un caractère public à l'attribution, le mécanisme n'est jusqu'à présent pas ou peu utilisé car il est mis en balance avec l'efficacité réelle des messages passés à titre confidentiel. Dans une matière aussi délicate, rendre public un nom c'est aussi prendre le risque de figer les positions et de compliquer l'engagement d'un dialogue. Mais je peux comprendre la frustration des parlementaires et du public face à cette apparente réserve dictée par l'efficacité.

Concernant le bon équilibre de nos moyens entre les dimensions défensives et offensives, une même discrétion rend peut-être ici moins visible l'ampleur des ressources déployées dans la seconde catégorie. La loi de programmation militaire prévoit bien des engagements sur ce point, rappelés encore récemment par la ministre. Le modèle français prévoit à cet égard une séparation spécifique entre les deux chaînes, qui doivent être bien articulées. » #

[...]

Trancheuse de câbles sous-marins. Ces câbles à très haut débit permettent de faire passer l'essentiel des communications internet mondiales
FRIFLASH/CC BY-SA 4.0

Extrait du rapport n° 7 (2019-2020) de Gérard LONGUET, fait au nom de la commission d'enquête du Sénat sur la Souveraineté numérique, déposé le 1er octobre 2019, «*Le devoir de souveraineté numérique – Tome II : comptes rendus*» : http://www.senat.fr/rap/r19-007-2/r19-007-21.pdf

Comment l’Europe tente d’enrayer la fuite de ses données

Colonisée depuis longtemps par les géants américains du numérique, l’Union européenne invoque la « souveraineté des données » pour tenter de reprendre le contrôle de ses « data », cet or noir du XXIe siècle, et de préserver la vie privée de ses citoyens.

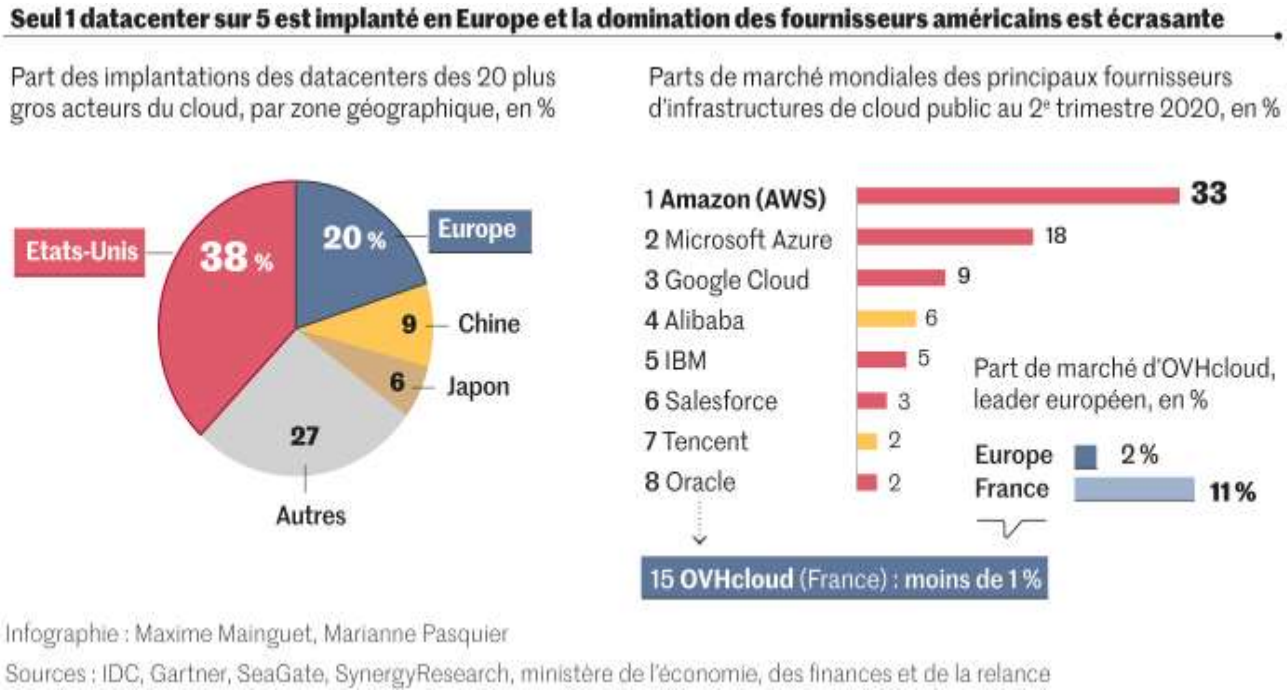
Par Charles de Laubier

Publié le 11 octobre 2020 à 18h00 - Mis à jour le 12 octobre 2020 à 05h46

Le commissaire européen au marché intérieur, Thierry Breton, présente la stratégie numérique de la Commission européenne, le 19 février. YVES HERMAN / REUTERS

L’Europe veut-elle en découdre avec les géants américains du numérique, comme tentent de le faire les trois voisins désemparés du film français *Effacer l’historique*, sorti cet été ? Ces derniers, d’anciens « gilets jaunes » qui se désolent de voir leurs vies privées prises au piège de la Toile et de leurs smartphones, décident de demander des comptes aux stars d’Internet.

Comme les personnages du film, le Vieux Continent entend lui aussi passer à l’offensive. La vie privée des internautes, leurs noms, adresses, téléphones, cartes de crédit et autres informations personnelles collectées par les réseaux sociaux ou les sites de commerce sont piégés dans d’immenses entrepôts d’ordinateurs formant le cloud, un nuage de centres de données disséminés dans le monde et détenus très majoritairement par des géants américains. Amazon Web Services (AWS), Microsoft (Azure), Google (Drive) et Apple (iCloud) détiennent à eux seuls plus de 70 % du marché des services d’hébergement massif de données, stockées en général aux Etats-Unis.



Cette dépendance préoccupe l'Europe, soucieuse de restaurer sa *« souveraineté numérique »*. Surtout lorsque les data exploitées sont sensibles. Karim Khelfaoui, un médecin exerçant à Marseille, s'est notamment révolté sur les réseaux sociaux en mai contre la collecte des données personnelles de santé de ses patients et de leurs proches. L'administration lui demande en effet, comme à tous les médecins, de les *« faire remonter »* à l'Assurance-maladie (la Sécurité sociale), afin d'envoyer, dans les foyers suspects ou ayant une personne positive au coronavirus, une *« brigade sanitaire »* pour lutter contre le Covid-19. *« Je suis médecin, pas flic !,* s'est insurgé Karim Khelfaoui. *Il est hors de question que je viole le secret médical et la confiance de mes patients. Surtout que leurs données de santé seront stockées sans leur consentement sur de nouveaux systèmes d'information, comme la plate-forme Health Data Hub, qui est hébergée par Microsoft. »*

Savoir où se trouvent leurs données personnelles est une question qui taraude les Européens. Mais elle reste souvent sans réponse, car ni les Gafam (Google, Apple, Facebok, Amazon, Microsoft) ni les entreprises en ligne ne sont tenus d'afficher le pays où ils les hébergent. *« Le responsable du traitement des données n'a pas l'obligation d'indiquer leur lieu d'hébergement et de stockage aux personnes dont les informations sont collectées. Pourtant, lorsque le serveur est localisé en dehors de l'Union européenne, ce serait une bonne pratique »,* souligne l'avocate Christiane Féral-Schuhl. En France, la loi dite « pour la confiance dans l'économie numérique » oblige depuis 2004 les sites Internet à mentionner les coordonnées de l'hébergeur. *« Mais l'adresse de l'hébergeur peut être distincte du pays de stockage »*, relèvent Sandra Tubert et Laura Ziegler, deux autres avocates.

Lieux de stockage inconnus

Le grand public, lui, craint pour sa vie privée. Et la 5G dont les enchères viennent d'être bouclées en France n'est pas près d'apaiser les esprits : *« Le déploiement massif d'objets connectés, allant de pair avec la 5G, participe de l'accaparement de données personnelles. On donne ainsi les clés d'un pouvoir de prévision et de contrôle social à des géants du numérique »*, se sont alarmés une soixantaine d'élus dans le *JDD* du 13 septembre. Le

scandale Cambridge Analytica – du nom de la société britannique qui a aspiré les données de près de 100 millions d'« amis » sur Facebook à des fins politiques – est devenu le symbole d'une Europe numérique aux allures de passoire. Ce qui a valu au réseau social, en 2019, une amende de 5 milliards de dollars (4,5 milliards d'euros) pour… négligence.

La firme de Mark Zuckerberg est en outre mise en cause depuis 2013 par un simple citoyen européen : Maximillian Schrems. Cet Autrichien avait saisi le régulateur irlandais afin d'empêcher le siège européen de Facebook à Dublin de transférer des données européennes vers les serveurs de sa maison mère aux Etats-Unis. La Cour de justice de l'UE a donné doublement raison à « Max » en annulant deux décisions majeures de la Commission européenne : les mal nommées « Safe Harbor », soit *« sphère de sécurité »* (invalidée il y a cinq ans), et « Privacy Shield », ou « bouclier vie privée » (invalidée en juillet dernier). Maximillian Schrems souhaite maintenant que l'Europe fasse respecter ce verdict par tous ceux qui font *« voyager les données »*.

Les particuliers, mais aussi les entreprises européennes, sont gagnés par le souci de la « territorialité des données », et les pouvoirs publics par leur « souveraineté ». Le problème est que les sites Internet ne savent pas toujours où ces données sont stockées. *« Une partie est stockée sur mon serveur, sur un site en France. Mais tous les logiciels qui sont en "léger", c'est-à-dire dans le nuage, sont gérés par leur éditeur et les données sont stockées dans un lieu que nous ne maîtrisons pas »,* constate Stéphanie Pauzat, dirigeante de Mil Eclair, une PME de nettoyage normande.

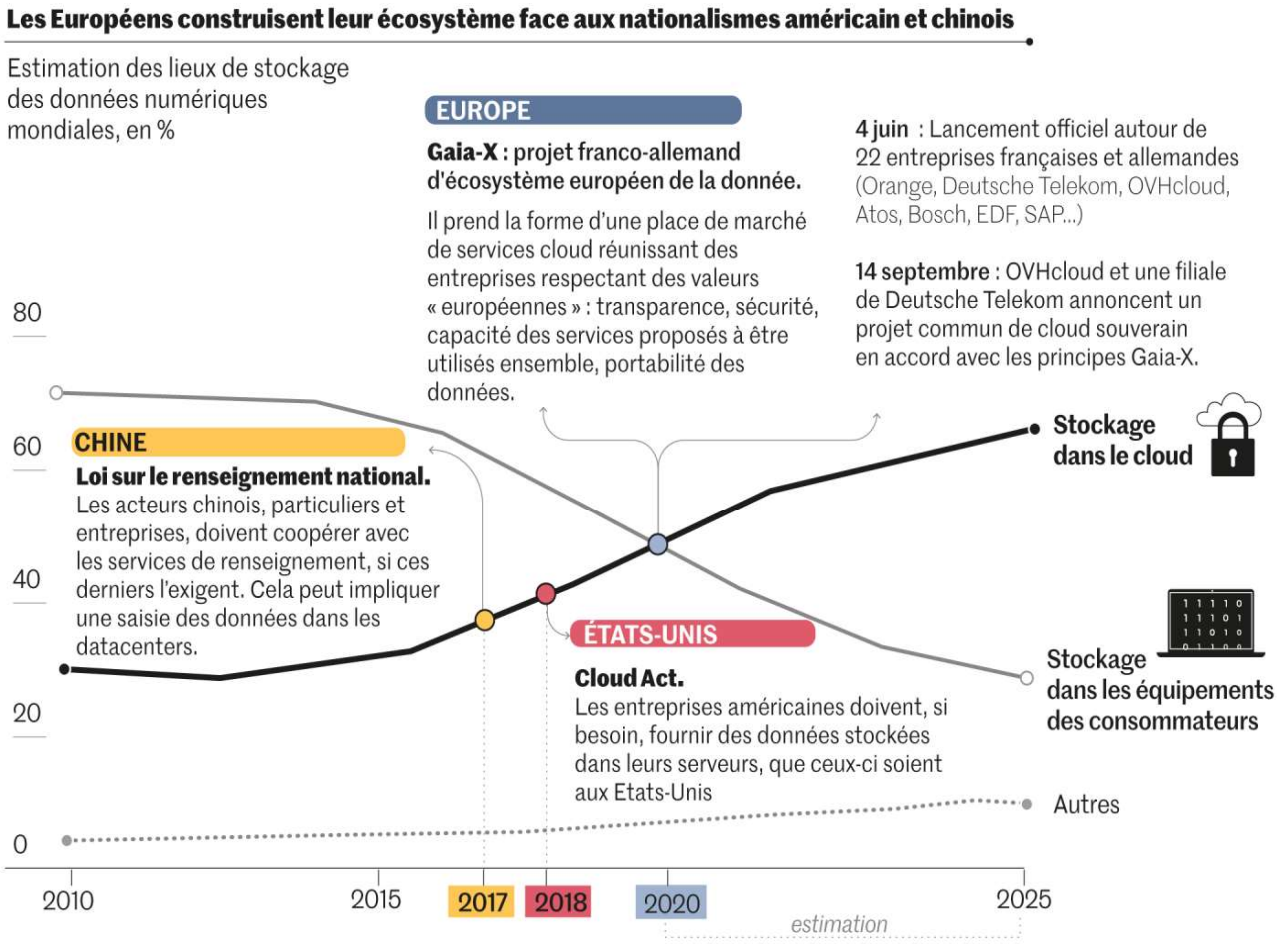
Du côté des grandes entreprises, pas facile d'y voir clair non plus. *« La plupart des grandes entreprises françaises ont des contrats avec des "hyperscalers" américains* [prestataires de traitement informatique massif pour le big data ou le cloud] *et il est difficile pour elles aujourd'hui de s'en affranchir. Peu sont d'ailleurs disposées à s'épancher sur leurs pratiques en la matière »,* confie un connaisseur des grandes organisations.

« Made in Europe »

Les administrations et les services publics montrent-ils la voie du rapatriement des données en France ou en Europe ? Membre du Club informatique des grandes entreprises françaises, la filiale Enedis d'EDF – gérant le réseau de distribution d'électricité – fait pour l'instant dans l'hébergement franco-français, y compris pour les données collectées par les fameux compteurs Linky : *« Nous stockons l'intégralité des données liées à notre activité sur nos propres serveurs, hébergés dans nos centres de données situés en France »,* précise Jean-Claude Laroche, directeur des systèmes d'information d'Enedis. Mais l'électricien ne devrait pas résister à l'appel du cloud puisque, *« à l'avenir »,* il est prévu d'y faire basculer les espaces collaboratifs tels qu'Office 365 de Microsoft.

Sa maison mère EDF fait partie de la vingtaine d'entreprises, dont Siemens, BMW, Safran, Bosch, Amadeus ou encore Orange, qui ont porté sur les fonts baptismaux le cloud franco-allemand Gaia-X : il s'agit de créer un « cloud souverain » européen pour protéger leurs données et être en conformité avec le règlement général sur la protection des données. *« En ce qui concerne les données à caractère personnel* (…)*, l'Europe a été trop lente et dépend désormais des autres »*, déplorait ainsi la présidente de la Commission européenne, Ursula von der Leyen, en dressant le 16 septembre l'état de l'Europe.

La société Gaia-X de droit belge a été créée en septembre. Première concrétisation de cette coopération entre Paris et Berlin : la cocréation d'un *« cloud public de confiance »,* confié au champion français, la société familiale OVHcloud (ex-OVH) basée à Roubaix, et à l'allemand T-Systems (filiale de Deutsche Telekom). La commercialisation du stockage « made in Europe » est prévue pour début 2021. En France, la plate-forme des données de santé Health Data Hub songe notamment à se rallier à Gaia-X. *« Nous restons à l'écoute des industriels pour anticiper la migration vers une autre solution d'hébergement, dès qu'une offre nationale ou européenne sera disponible »*, indique Stéphanie Combes, directrice de ce groupement d'intérêt public.



Infographie : Maxime Mainguet, Marianne Pasquier
Sources : IDC, Gartner, SeaGate, SynergyResearch, ministère de l'économie, des finances et de la relance

Depuis son lancement en décembre 2019, cette plate-forme est non seulement alimentée par les médecins, mais aussi par les pharmacies, les laboratoires d'analyse ou encore les cardiologues. Ces données de santé sont censées être pseudonymisées avant d'être hébergées chez Microsoft. Mais où ? *« Elles sont actuellement stockées dans les centres de données de Microsoft aux Pays-Bas. D'ici à la fin de l'année, elles le seront toujours chez Microsoft, mais en France »,* promet Stéphanie Combes. La Commission nationale de l'informatique et des libertés doit rendre un avis sur un projet de décret sur le fonctionnement de cet entrepôt de données de santé, dont elle souhaite que le stockage reste en Europe. Le Conseil d'Etat, lui, a rejeté par deux fois des recours contre ce transfert vers Microsoft.

« Patriotisme numérique »

La transformation numérique de l'Etat français est aussi l'occasion de relocaliser des données. La direction interministérielle du numérique, à l'origine du portail FranceConnect, utilisé par 17 millions de Français pour leurs démarches administratives, prône ainsi des *« espaces souverains de stockage, associés à des services publics de qualité »*. Son directeur, Nadi Bou Hanna, l'assure : *« Ces données sont stockées par défaut en Europe, et dans la plupart des cas par l'administration française. »*

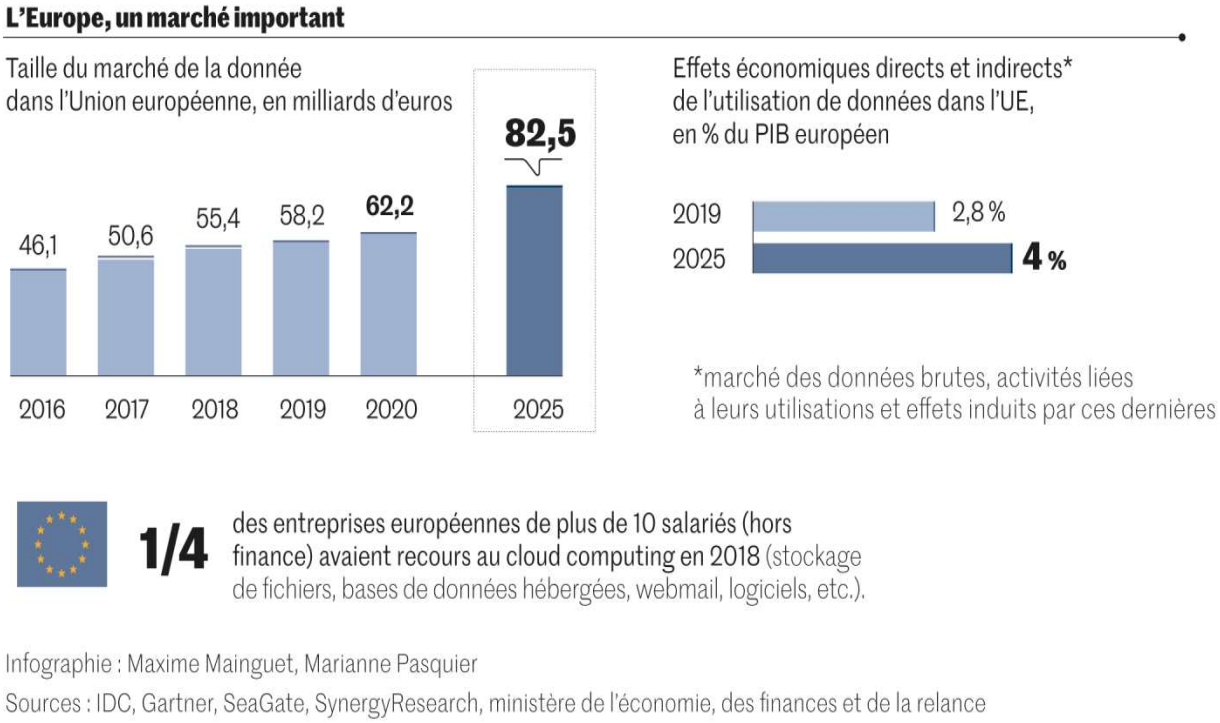
Des Etats sont même tentés par la « nationalisation des données » de leurs services publics. Mais, lancées il y a dix ans par le gouvernement en France, les sociétés Cloudwatt et Numergy – respectivement absorbées par Orange et SFR – ont été des échecs. *« Ils avaient un positionnement strictement national ; leur marché était beaucoup trop limité »,* explique Helmut Reisinger, directeur général d'Orange Business Services (OBS). *« Il y avait un manque de sponsors de l'Etat français, pour encourager les acteurs français »,* regrette Christophe Delaye, directeur exécutif réseaux et systèmes d'information chez SFR.

Aujourd'hui, faire du stockage de données un enjeu de « souveraineté nationale », voire de « patriotisme numérique », prend de l'ampleur partout dans le monde. Les Etats-Unis soupçonnent par exemple le réseau social des ados TikTok, dont les données sont stockées en Virginie et à Singapour, de cyberespionnage au profit de son pays d'origine, la Chine – à l'instar de Huawei. Pourtant, le pays de l'« America First » est lui-même un expert en surveillance de masse avec ses programmes Prism (dont les abus ont été révélés en 2013 par le lanceur d'alerte Edward Snowden) et Upstream, tous deux autorisés par la loi américaine FISA.

En Chine, une loi sur la cybersécurité impose quant à elle que les plates-formes étrangères stockent les données des Chinois au sein de l'empire du Milieu. Idem en Russie pour les données des Russes. Et, en Europe, les Big Tech américaines, déjà suspectées d'évasion fiscale, veulent éviter d'être accusées d'« évasion de données » au profit des Etats-Unis. Amazon veut rassurer : *« Les clients français déterminent la région où leurs données sont stockées, y compris en France depuis 2017. Ils peuvent aussi crypter leurs données et gérer leurs clés de chiffrement »,* indique Stephan Hadinger, directeur de la technologie chez AWS France. Cette filiale d'Amazon est membre de l'association bruxelloise Cispe, elle-même cofondatrice de Gaia-X. Le loup dans la bergerie ?

Un parapluie suffisant ?

« Les fournisseurs européens sont en retard de floraison », déplore Henning Kagermann, ancien coprésident de la société allemande SAP. Dans un rapport publié en juillet, il plaide donc pour la création d'une *« sphère publique européenne »* englobant les services publics. A Bruxelles, on pose les jalons d'un cloud souverain, que le commissaire européen Thierry Breton a surnommé « Gaia-UE » : *« Nous avons annoncé un investissement de 2 milliards d'euros pour la mise en place du projet. Les premiers appels à manifestation d'intérêt seront lancés d'ici à la fin de l'année »*, affirme-t-il.



Reste à savoir si la souveraineté est un parapluie suffisant pour empêcher que les nuages américains – rejoints par les chinois Alibaba, Tencent ou encore Huawei – ne fassent la pluie et le beau temps sur les données des Vingt-Sept. Pour Helmut Reisinger, chez Orange, partie prenante de Gaia-X, *« il ne s'agit pas de recréer un Gafam européen ». « Pourquoi devrions-nous nous résoudre à devenir la colonie numérique de la Chine ou des Etats-Unis ? »,* se rebiffe quant à lui Michel Paulin, directeur général d'OVHcloud.

Mais les Américains ne seront pas pour autant évincés du marché unique numérique, pas plus qu'ils ne le seront du futur *« marché unique des données »* (industrielles, financières, etc.). Pour Cédric O, secrétaire d'Etat au numérique*, « à aucun moment, il n'a été envisagé de se passer des offres proposées par les grands acteurs du numérique, essentiellement américains. Les projets de cloud souverain et Gaia-X sont complémentaires, imbriqués »*. Il inaugurait mi-septembre à Paris le salon Big Data, dont les données collectées sont hébergées chez OVHcloud et… Amazon.

Charles de Laubier

FIC 2020 : Vers une cybersécurité souveraine en France et en Europe (extraits)

Jacques Cheminat, publié le 29 Janvier 2020

Les discours inauguraux de l'édition 2020 du FIC à Lille ont clairement mis l'accent sur la structuration de la filière cybersécurité en France et plus globalement en Europe. En toile de fond, la souveraineté des Etats et les rapports de force dans le monde cyber. (…)

En direct de Lille. Le Forum international de la cybersécurité (FIC) a ouvert ses portes à Lille. Rendez-vous incontournable pour la profession, il attendait cette année 12 000 personnes. Si la thématique de l'événement porte sur la place de l'humain dans la cybersécurité, les discours inauguraux ont surtout montré les forces de la filière et son impact géopolitique.

Le directeur de la gendarmerie nationale, le Général Christian Rodriguez, a bien sûr vanté les mérites du C3N (centre de lutte contre les criminalités numériques) et des enquêteurs spécialisés N-Tech. Ils ont été confrontés à 89 000 infractions liées au numérique en 2019, soit une hausse de 20%. Parmi les nouveautés annoncées, il a évoqué la création d'une plateforme d'investigation sur les objets connectés du quotidien. De même, des enquêteurs vont s'occuper des cryptoactifs avec le développement des cryptomonnaies. « Il faut s'adapter pour être capable de détecter, d'identifier, d'analyser et de remonter les attaques », souligne le dirigeant toute en restant attentif « aux nouvelles frontières de la sécurité comme les algorithmes ». (…)

Gallia, une plateforme collaborative pour la filière cybersécurité

Autre acteur important, Hexatrust avec son président Jean-Noël de Galzain, ardent promoteur des entreprises de la filière. En charge du projet « cybersécurité et sécurité de l'IoT » du comité stratégique de filière industries de sécurité, il a annoncé au FIC le lancement « de la première plateforme communautaire destinée à fédérer les acteurs de la cybersécurité française ». Cette initiative se nomme GALLIA et entend réunir des personnes de différents horizons (administrations, associations d'industriels et d'utilisateurs, clusters, pôles, campus, écoles communautés d'experts…). L'objectif est de pouvoir échanger en mode collaboratif sur des projets, des bonnes pratiques et des opportunités.

Guillaume Poupard, directeur général de l'ANSSI (agence nationale de la sécurité des systèmes d'information), considéré par certains comme le capitaine de l'équipe de France de la cybersécurité, a rappelé le contexte géopolitique de la filière cybersécurité. « Il existe fondamentalement deux cercles. Le premier est celui des cyber-puissances où quelques Etats ont une volonté de supériorité et un second cercle où des Etats visent la suprématie ». Pour lui, la France doit se situer « dans le premier cercle » et d'ajouter, « nous ne voulons pas chercher un protecteur, être inféodé ». Cette posture implique pour lui un effort à deux niveaux : européen et national.

Une souveraineté numérique européenne et française assumée

Sur le premier point, « la souveraineté cyber de l'Union Européenne n'est plus un gros mot », constate le dirigeant. « L'Europe est devenue un lieu commun pour parler de la souveraineté, la construire, sur des valeurs éthiques, sur la liberté individuelle, sur une vision du monde différente », reconnait-il. Cela se traduit par des initiatives comme le Cyber Act, la directive NIS, l'ENISA ou des prises de position de la Commission européenne sur la 5G. « Les Etats membres se sont fédérés pour réaliser une analyse de risque commune et l'exécutif européen propose une boîte à outils pour le déploiement de la 5G », glisse Guillaume Poupard. Pour lui, « la 5G doit être un réseau fiable et sûr, c'est un sujet d'infrastructure critique et il y aura certaines exigences. Par exemple, pour les cœurs de réseaux qui sont sensibles, le choix d'un acteur européen (NDLR : Nokia ou Ericsson) sera privilégié, de même que dans certains lieux géographiques sensibles comme les capitales, le centrales nucléaire, les zones militaires ». En dehors de ces premiers pas vers une souveraineté numérique européenne, il reste des efforts à mener, constate le directeur de l'ANSSI. « Aujourd'hui, la coordination entre Etats membres en cas d'attaques n'est pas prête, mais les choses avancent ».

Enfin, le match de la souveraineté se joue aussi sur le territoire national. « L'équipe de France travaille avec les différents acteurs depuis plusieurs années avec un pack régalien invisible, mais efficace et un partenariat public-privé solide », constate le patron de l'ANSSI. Si équipe il y a, faut-il encore qu'il y ait un terrain d'entraînement et un terrain d'honneur. Pour cela, il pousse l'initiative du Campus cybersécurité porté par Michel Van Den Berghe, directeur général d'Orange Cyberdéfense. « Nous avons vraiment besoin d'un lieu sur Paris, car le lien entre les différents acteurs de la cybersécurité manque terriblement », conclut Guillaume Poupard.

N° 7

SÉNAT

SESSION ORDINAIRE DE 2019-2020

Rapport remis à M. le Président du Sénat le 1er octobre 2019

Enregistré à la Présidence du Sénat le 1er octobre 2019

RAPPORT

FAIT

au nom de la commission d'enquête (1) sur la **souveraineté numérique***,*

Président

M. Franck MONTAUGÉ,

Rapporteur

M. Gérard LONGUET,

Sénateurs

Tome I : Rapport

(1) Cette commission est composée de : M. Franck Montaugé, *président* ; M. Gérard Longuet, *rapporteur* ; M. Patrick Chaize, Mmes Sylvie Robert, Catherine Morin-Desailly, MM. Yvon Collin, M. André Gattolin, MM. Pierre Ouzoulias et Jérôme Bignon, *vice-présidents* ; Mme Viviane Artigalas, MM. Jérôme Bascher, Bernard Bonne, Mme Martine Filleul, MM. Christophe-André Frassa, Loïc Hervé, Laurent Lafon, Rachel Mazuir, Stéphane Piednoir, Mmes Sophie Primas, Frédérique Puissat et M. Hugues Saury.

PRINCIPALES RECOMMANDATIONS

La souveraineté nationale fonde le pacte républicain, pacte par lequel le citoyen accepte une discipline collective fondée sur la loi, en contrepartie d'une protection.

La souveraineté nationale, pour ne remonter qu'à la fondation de la République en septembre 1792, n'a jamais été certaine, quelle que soit la nature des défis qu'elle devait affronter.

Aujourd'hui, la question de la souveraineté numérique est totalement actuelle, car si l'ère numérique est à la fois une chance et une certitude partagée dans le monde entier, elle

constitue pour la France, comme pour les pays de l'Europe, un triple défi éthique, de sécurité et de liberté économique.

D'abord, en effet nos sociétés sont confrontées à une mise en cause sourde de leurs valeurs : l'homme est moins un citoyen et un sujet de droit, mais de plus en plus une somme de données à exploiter. Ce n'est pas notre conception de la personne humaine, ce n'est pas non plus le modèle de société que nous portons et dans lequel s'incarnent nos valeurs de respect de tous et de chacun. La souveraineté numérique est donc la condition nécessaire et indispensable à la préservation de ces valeurs.

Des actions ont été entreprises depuis plus de 15 ans pour la restaurer ou la préserver. Point cependant de stratégie globale lisible qui fédèrerait les énergies et les efforts. Votre commission d'enquête souhaite y remédier en proposant :

- un principe et une méthode :

o le principe est que la souveraineté numérique est un devoir national et, à ce titre, engage nos compatriotes, toutes responsabilités confondues ; aussi serait mis en place un « Forum national du numérique », structure temporaire qui permettrait de donner le coup de collier nécessaire pour sortir de la situation peu satisfaisante dans laquelle les attributs traditionnels de la souveraineté nationale et nos valeurs démocratiques sont malmenés ;

o la méthode serait la présentation par le Gouvernement et l'adoption par le Parlement d'une loi d'orientation et de suivi de la souveraineté numérique (LOSSN). La discussion parlementaire et le vote d'une loi d'orientation triennale permettront au Parlement d'exercer pleinement son rôle de gardien de la souveraineté numérique nationale.

Cependant, dès maintenant, des mesures précises et urgentes dans le domaine de la protection des données, une réforme de la réglementation visant le renforcement de notre souveraineté numérique et une action sur les leviers de l'innovation et du multilatéralisme doivent être menées.

1. Définir une stratégie nationale numérique au sein d'un Forum institutionnel temporaire du numérique

La stratégie gouvernementale pour la défense de la souveraineté numérique est dispersée entre souveraineté et libertés publiques, sécurité et défense, et présence économique effective sur un marché nécessairement mondial, ce qui la rend peu lisible. Les ministères et grands opérateurs publics doivent impérativement mieux articuler leurs efforts et leurs actions en faveur de la souveraineté numérique, posée comme un enjeu fédérateur. Il convient d'associer à cette réflexion les collectivités territoriales, responsables de l'aménagement numérique du territoire, la recherche et l'industrie, le public et le privé.

Nous avons, au cours de nos travaux, constaté qu'il manquait, au-delà des actions menées, engagées ou projetées, une impulsion fédératrice. Ce n'est ni un secrétaire d'État au numérique, ni le Gouvernement, ni l'industrie, ni les prestataires de service qui peuvent seuls définir la stratégie nationale numérique dont notre pays a besoin. C'est grâce à un travail collectif, alliant les forces et expériences de chacun, et s'appuyant sur l'excellence de la recherche française, sur l'inventivité de nos territoires, sur l'exigence des associations de

défense des citoyens, sur le dynamisme des fleurons économiques français, qu'il sera possible de mobiliser nos forces, et elles sont réelles, au service de notre souveraineté numérique.

Nous proposons la transformation du Conseil national du numérique en un Forum de concertation temporaire, force de propositions et d'impulsions fédératrices, pour renforcer l'approche transversale et interministérielle du numérique. D'une durée de vie limitée à deux ans, il permettrait au Gouvernement et au Parlement de réaliser les arbitrages nécessaires à la défense de notre souveraineté numérique.

2. Inscrire l'effort pour la souveraineté numérique dans le temps en votant une loi d'orientation et de suivi de la souveraineté numérique (LOSSN)

Une loi d'orientation et de suivi de la souveraineté numérique devrait découler des travaux du Forum : à l'image de la loi de programmation militaire, elle garantirait davantage de lisibilité et de stabilité aux entreprises, et mettrait en oeuvre un pilotage public plus rigoureux des innovations dans les secteurs et technologies essentiels à la défense de la souveraineté numérique française. Le suivi de l'exécution de la LOSSN par le Parlement garantirait la gestion politique de ces choix stratégiques. Le Parlement s'exprimerait à cet effet de manière régulière.

Cette loi, triennale, définirait une stratégie claire sur les infrastructures du numérique avec deux piliers urgents : l'attractivité de notre territoire pour les câbles sous-marins, les centres de données et la fibre optique, et l'accélération de la couverture numérique du territoire. Elle favoriserait également les technologies numériques d'avenir et les domaines dans lesquels la France a une carte à jouer pour devenir un leader européen et mondial. Ces domaines, définis dans le cadre du Forum, ne se résumeraient pas aux seules technologies de rupture, mais viseraient également le développement des hautes technologies dans lesquels le savoir-faire français est déjà reconnu et incarné par de grandes entreprises françaises dont le rachat, qui plus est, est peu envisageable contrairement à celui de start-up innovantes.

Cette loi inclurait le financement de solutions répondant aux attaques qui visent notre modèle de société et qui fragilisent notre souveraineté : fournir une carte d'identité électronique ; *élaborer une cryptomonnaie publique sous l'égide de la Banque centrale européenne et à laquelle pourraient collaborer les banques centrales des pays non membres de la zone euro (ex. Suisse, Royaume-Uni, Suède, Danemark)* ; obtenir au sein de l'OCDE une taxation commune des multinationales du numérique, avec un principe d'imposition fondé sur le lieu de consommation ; généraliser la solution de la banque centrale européenne pour les paiements transfrontières.

3. Protéger les données personnelles et les données économiques stratégiques

Cet objectif se déclinerait en deux grands axes :

Restituer à chacun la maîtrise de ses données

Sur la base d'un premier bilan du droit à la portabilité des données personnelles (existant depuis la loi « République numérique » et consacré par le RGPD), il conviendrait de soutenir et d'étudier la faisabilité technique et opérationnelle d'une obligation d'interopérabilité (bénéfices, coûts, impact sur le consommateur et l'innovation), y compris comme mesure de régulation asymétrique imposée aux grandes plateformes systémiques, le Gouvernement

associant les régulateurs nationaux (ADLC, CNIL) et présentant au Parlement la position qu'il compte défendre au niveau européen sur ce sujet central pour nos concitoyens.

Défendre les données stratégiques de nos entreprises contre l'application de lois à portée extraterritoriales

Une obligation de localisation des données sur le territoire national peut être justifiée par des motifs de sécurité publique, mais ce n'est qu'une solution imparfaite ; il convient de cartographier et de faire émerger des solutions pour l'hébergement et le stockage des données sensibles autour de prestataires français et européens non soumis aux législations étrangères à portée extraterritoriale.

Parallèlement, il est essentiel d'opposer fermement notre législation nationale et européenne au *Cloud Act* ou à toutes autres normes se voulant porteuse d'un ordre juridique extraterritorial. La loi dite de « blocage» doit être renforcée, sur la base de rapport du notre collègue député Raphaël Gauvain afin que les entreprises françaises ne soient plus démunies face aux procédures américaines, notamment (mise en place d'une déclaration aux autorités françaises, accompagnement par une administration dédiée et durcissement des sanctions encourues).

S'il convient d'encourager la conclusion rapide d'accords de coopération entre l'Union européenne, ses États membres et les États-Unis dans le cadre du *Cloud Act*, il faut aussi réfléchir à l'opportunité d'étendre les sanctions prévues par le RGPD aux données non personnelles stratégiques des personnes morales, pour sanctionner les intermédiaires qui transmettraient aux autorités étrangères des données en dehors de ce mécanisme d'entraide administrative ou judiciaire.

4. Adapter la réglementation aux défis numériques

Cet objectif se déclinerait en quatre grands axes :

Muscler le droit de la concurrence aux niveaux national et européen

Le droit de la concurrence n'est plus adapté aux spécificités de l'économie numérique et devrait, par conséquent, être amendé. Il faut faciliter le recours à des mesures conservatoires, lorsque l'urgence le justifie, et réviser le champ de contrôle des concentrations, par exemple en introduisant un nouveau seuil basé sur la valeur de rachat. Enfin, la France doit transposer au plus vite la directive ECN +, qui permet aux autorités de prononcer des injonctions structurelles (ex. cession d'une branche) dans le cadre des sanctions en cas de pratiques anticoncurrentielles.

Utiliser l'information : la « régulation par la donnée »

Les autorités de régulation souhaitent réguler par la donnée, c'est-à-dire s'appuyer sur la puissance de l'information pour réguler le marché. Il s'agit de collecter les informations de toute origine, y compris citoyenne, pour détecter les signaux faibles et les risques systémiques. L'analyse de ces données permet ensuite de mieux éclairer les choix des acteurs publics et des utilisateurs, et d'anticiper les réactions négatives de ces derniers. Le but de cette approche est moins de sanctionner les entreprises concernées que d'orienter le marché. Pour ce faire, les autorités de régulation doivent se doter des compétences, humaines et

technologiques, nécessaires. La démarche concertée présentée le 8 juillet 2019, de plusieurs régulateurs (l'Autorité de la concurrence, l'AMF, l'Arafer, l'Arcep, la CNIL, la CRE et le CSA) en ce sens est un premier pas décisif qui doit être soutenu.

Étudier la faisabilité de nouvelles régulations sectorielles...

Ces nouvelles régulations sectorielles incluraient, après étude d'impact et de faisabilité, la neutralité des terminaux, l'accès sous le contrôle du régulateur aux données essentielles à l'exercice d'une activité, la transmission des informations pertinentes des plateformes aux autorités publiques ou encore l'accès aux méthodes et données sous-jacentes des algorithmes.

Donner accès à certaines données permet en effet de favoriser la concurrence et l'innovation. Dans ce cadre, les entreprises devraient être incitées à partager et à mutualiser leurs données privées, avec l'État comme tiers de confiance. Sur l'ouverture des données, l'approche ne peut être globale et la décision doit être prise au cas par cas.

...voire d'obligations proactives, spécifiques et multisectorielles pour les acteurs systémiques du numérique : la régulation « ex-ante ».

Identifier les acteurs essentiels du numérique pourrait se faire grâce à un faisceau d'indices permettant de définir leur caractère « systémique »[1](*). De nouvelles obligations applicables à ces acteurs numériques systémiques pourraient être définies de façon proactive. Les pistes retenues par votre commission d'enquête portent sur la mise en oeuvre d'une obligation de transparence de l'activité et d'une obligation de ménager dans des conditions équitables l'accès d'autres acteurs pour certains types de données. De même, le renforcement de la portabilité des données et de l'interopérabilité des plateformes doit être recherché. L'auditabilité et la redevabilité[2](*) des algorithmes utilisés doivent être des objectifs du législateur. Cela suppose de permettre l'accès des chercheurs ou d'organismes publics à ces algorithmes pour évaluer et garantir leur transparence, leur intelligibilité, leur conformité à la loi, la non-discrimination, et leur loyauté.

5. Utiliser les leviers de l'innovation et du multilatéralisme

Cet objectif se déclinerait en deux grands axes :

Encourager les innovations aux niveaux national et européen

Sans innovation, pas de souveraineté numérique. Des pistes existent pourtant pour améliorer notre pilotage des innovations, pour attirer le capital financier nécessaire et pour favoriser les liens entre entreprises et recherche privée : revoir, au niveau européen, le régime des aides d'État ; utiliser le levier de l'achat public; élargir la dépense fiscale IR-PME pour soutenir le capital-risque ; clarifier les conditions du crédit d'impôt recherche pour les entreprises du secteur numérique ; créer un portail unique permettant aux entreprises de visualiser l'ensemble des dispositifs existants ; renforcer la place des entreprises au sein des centres de recherche publics.

Porter la vision française de la souveraineté numérique dans les enceintes multilatérales

Alors que sa souveraineté est concurrencée, la France doit défendre sa présence au sein des organismes internationaux. À ce titre, renforcer la mobilisation des acteurs français et

européens du numérique dans les organismes de normalisation multilatéraux est une action prioritaire. Les désengagements récents, qui semblent presque fortuits, sont signes de l'absence de pilotage d'une stratégie nationale de préservation de la souveraineté numérique nationale. Le réinvestissement des agoras de normalisation est indispensable.

De même, la promotion à l'international de la vision française de cybersécurité se décompose en deux items : le droit international est applicable au cyberespace, et l'attribution d'une cyberattaque est une décision politique souveraine et ne peut être faite par une structure multinationale, qu'elle soit interalliée comme l'OTAN ou autre. La défense de ce principe est essentielle à la pleine restauration de notre souveraineté numérique.

Le Figaro

L'armée française sécurise une pépite de la tech convoitée par la CIA

RÉCIT - Visée par In-Q-Tel, le fonds de la CIA, Preligens, leader de l'analyse de données à base d'IA, reste français.

Par Véronique Guillermard
Publié le 19/11/2020 à 16:53

La France veut protéger ses pépites technologiques. La décision du ministère des Armées d'investir, via son fonds DefInvest, dans la start-up tricolore Preligens (ex-Earthcube), va dans ce sens. La jeune pousse, leader dans l'analyse de données satellitaires, à base d'Intelligence artificielle (IA), pour le compte des services de renseignement et des armées, vient de lever 20 millions d'euros auprès de trois fonds. L'opération, pilotée par Ace Management, voit aussi entrer des business Angels tel qu'Octave Klaba, président fondateur de l'hébergeur OHV Cloud, à titre personnel.

À l'issue de l'opération, le capital de Preligens reste 100% français. Les deux fondateurs - Arnaud Guérin, PDG, et Renaud Allioux, directeur de la technologie -, conservent plus de 50% des parts. Le solde se partage entre des investisseurs privés ainsi que trois fonds, Ace Management, DefInvest et 360 Capital, qui accompagnent la jeune entreprise depuis ses débuts en 2016.

Courtisé par le fonds de la CIA

« *Nous avons décidé d'investir dans Preligens en raison de ses compétences uniques dans le traitement automatisé et l'analyse d'images satellitaires à base d'IA et dans le machine learning, qui sont d'un grand intérêt pour les services de renseignement et les forces armées* », explique-t-on au cabinet de Florence Parly, la ministre des Armées. Preligens s'appuie sur les images collectées par les satellites CSO notamment. *« Les applications de cette pépite nationale sont primordiales pour le domaine de la défense »*, a déclaré Florence Parly lors d'un déplacement chez Preligens. *« Elles nous apportent un vrai gain opérationnel pour l'exploitation de nos informations géospatiales: sans Preligens nous ne verrions pas certaines choses »*.
Cet éditeur de logiciels a acquis une compétence pointue dans la détection d'éléments pertinents au sein de masses de données gigantesques. Cela, de façon automatique et très rapide. Ses algorithmes apportent ainsi une aide précieuse aux analystes spécialisés pour exploiter les informations pertinentes dans le cadre de missions de surveillance et/ou d'intervention sur le terrain.
Preligens restera donc français alors qu'elle était courtisée par In-Q-Tel, le fonds de la CIA, qui avait très vite vu tout l'intérêt de faire basculer cette pépite tricolore sous capitaux américains. D'autant que Preligens a déjà gagné des contrats aux Etats-Unis, notamment avec les forces spéciales. *« Nous réalisons 50% de notre chiffre d'affaires à l'international dans cinq pays où nous avons remporté des marchés, notamment auprès de l'OTAN, de l'Union européenne, du Royaume-Uni et des États-Unis. Nous avons démontré qu'il n'est pas obligatoire*

d'internationaliser le capital pour se développer hors de France », explique Arnaud Guérin, dans un entretien du Figaro.

Déploiement dans 10 pays supplémentaires

Face au risque de captation du savoir-faire technologique de Preligens, le Ministère des Armées a donc réagi. La Direction générale de l'armement (DGA) avait repéré la start-up dès 2017. Elle l'a aidé à accéder, par deux fois, à des fonds, dans le cadre du mécanisme de subvention publique Rapid. Preligens a également été sélectionnée pour développer des briques technologiques basées sur l'IA dans le cadre du projet « Man Machine Teaming » (relation homme-machine) à bord de l'avion de combat du futur.

Preligens va utiliser les fonds levés afin de booster son activité historique d'analyse de données géospatiales. Cela, en poursuivant le déploiement de ses solutions sur les bases militaires françaises. Trois sites pilotes en opération les utilisent déjà. Une trentaine de sites de défense doivent s'équiper dans les prochains mois.

Parallèlement, la start-up va accélérer son internationalisation. *« Dans les 18 prochains mois, nous ciblons 10 pays supplémentaires en Europe, en Amérique du Nord et en Asie, en s'appuyant les relais internationaux de la DGA ainsi que sur des partenariats avec des industriels »*, précise Arnaud Guérin. En octobre dernier, Preligens a par exemple noué un partenariat avec Airbus Defence & Space, afin de proposer un nouveau service de surveillance de sites militaires sensibles et en opérations extérieures en s'appuyant sur les images collectées par les satellites d'Airbus, partenaire clef des armées.

Lutte contre le terrorisme

Enfin, la jeune pousse va investir dans le développement de nouveaux logiciels afin d'élargir l'éventail de ses services. *« Nous ne traiterons plus seulement des images satellites mais aussi des données collectées par des drones et des avions mais aussi d'autres sources, notamment électromagnétiques, mais aussi des messages texte, sous documents Word ou sur les réseaux sociaux ainsi que sur le web »*, développe le PDG de Preligens. A cet effet, l'entreprise va recruter une centaine de personnes d'ici à fin 2021, afin de porter ses effectifs à 180.

Ces nouvelles compétences génèreront des services très utiles aux services de renseignements, de contre-terrorisme, de lutte contre les trafics de stupéfiants ou encore contre la prolifération.

Le Figaro

La France mise 500 millions pour protéger ses start-up de l'appétit des Gafa

Bruno Le Maire et Cédric O vont présenter un plan destiné à préserver la souveraineté nationale dans le numérique, dont le montant total s'élève à 1,2 milliard d'euros.

Par Elsa Bembaron et Guillaume Guichard
Publié le 04/06/2020 à 18:53, Mis à jour le 05/06/2020 à 10:06

Info le Figaro. La crise de la Covid-19 fait revenir sur le devant de la scène les enjeux liés à la réindustrialisation, au renforcement du tissu économique local et à la souveraineté nationale. Or, dans certains domaines, la France, pays aux 13.000 start-up, disposent de pépites qui sont autant de «proies», pouvant être rachetées par des géants du numériques extra-territoriaux, essentiellement américains.

Pour préserver les start-up de l'appétit de conquête des Gafa, le ministre de l'économie Bruno Le Maire et le secrétaire d'Etat au numérique Cédric O, vont annoncer une série de mesures, pouvant atteindre 500 millions d'euros. Un fonds de souveraineté, qui devrait être doté de 150 millions d'euros et pourrait atteindre 500 millions d'euros dès 2021 sera mis en place, selon nos informations.

BPIfrance à la manoeuvre

Géré par Bpifrance, il aura pour objectif premier de préserver la souveraineté nationale, via des prises de participations minoritaires dans des entreprises stratégiques. Le champ couvert par cette définition pourrait néanmoins être assez large, allant de start-up développant des services Cloud, à des BioTech en passant par l'éducation, la Défense, les énergies renouvelables…

A cela devrait s'ajouter le doublement du French Tech Bridge, le programme de prêt-relais de Bpifrance destiné à aider les entreprises à faire face à leurs difficultés de trésorerie, liées à la crise. Le dispositif atteindra 160 millions d'euros. A cela s'ajoute une offre de prêts de 100 millions d'euros pour les entreprises qui ne peuvent pas accéder au PGE bien qu'étant en difficulté, une demande du secteur depuis le début de la crise.

De plus, un nouveau fonds de 200 millions pour « soutenir l'émergence d'un nouveau vivier de start-ups » est créé, en faveur de ces jeunes chercheurs qui veulent se lancer dans l'aventure entrepreneuriale. La deep tech profitera également d'un second fonds French Tech Acceleration, doté de 100 millions d'euros.

Ces annonces, dont le total atteint 1,2 milliard d'euros - en y ajoutant d'autres petits gestes très ciblés - s'inscrivent dans un plan global de défense de la souveraineté nationale et survient après le présentation officielle, jeudi, du projet Gaia-X de cloud souverain franco-allemand.

LA TRANSFORMATION NUMÉRIQUE DU MINISTÈRE DES ARMÉES

Arnaud Coustillière

La Découverte | « Hérodote »

2020/2 N° 177-178 | pages 165 à 177

ISSN 0338-487X
ISBN 9782348060250

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-herodote-2020-2-page-165.htm

La transformation numérique du ministère des Armées

Arnaud Coustillière[1]

Le constat s'impose depuis quelques années : le numérique est devenu un espace stratégique et a envahi tous les autres domaines conventionnels. Sur les théâtres d'opérations militaires, garantir une supériorité opérationnelle et, plus largement, une autonomie stratégique suppose une maîtrise du numérique qui nécessite la transformation numérique (TN) des armées. La TN est une nouvelle façon d'aborder le système d'information (SI) en mettant l'utilisateur et la donnée au centre afin de rendre le fonctionnement de l'organisation plus efficient. Ce défi passe entre autres par la numérisation des champs de bataille et par l'exploitation des données qui en sont issues. La transformation porte également sur l'efficience et la modernisation des métiers du ministère des Armées, la logistique, les ressources humaines (RH) et autres tâches administratives pour lesquelles un rattrapage numérique s'impose.

Constituant un des accélérateurs majeurs de la transformation numérique (TN), les technologies du numérique ont fortement évolué notamment sous les effets de l'augmentation des capacités de calcul et des capacités de stockage, des techniques de traitement de données de masse (TDM, aussi appelé *big data*) et de celles d'apprentissage qui ont permis un réel essor de l'intelligence artificielle (IA), et des objets connectés. Des applications civiles performantes sont déjà disponibles dans les domaines de la reconnaissance d'images y compris sur les réseaux sociaux, de la reconnaissance vocale, de la traduction automatique, du commerce électronique ciblé, sous l'impulsion des GAFAMI (grandes plateformes du Web

1. Vice-amiral d'escadre. Directeur général du numérique et des systèmes d'information et de communication (DGNUM) du ministère des Armées.

Google-Apple-Facebook-Amazon-Microsoft-IBM). De nombreux experts s'accordent sur le caractère structurant de l'IA dans l'évolution de nombreux secteurs économiques. Ces technologies sont des opportunités pour l'amélioration des performances opérationnelles et pour la transformation des activités organiques du ministère. Leur utilisation est une nécessité pour conserver l'ascendant face à nos adversaires potentiels et constitue un moyen d'apporter des services nouveaux et de l'efficacité à l'ensemble du personnel du ministère.

Le système d'information (SI) du ministère des Armées a entamé depuis deux ans une mutation visant d'une part à mieux intégrer les besoins des utilisateurs en se mettant à leur place dans une démarche de « parcours usager » et d'autre part à valoriser ses données. Il s'agit de mettre le SI en posture d'affronter et de s'adapter à la révolution numérique qui imprime son propre tempo.

Face à ces (r)évolutions technologiques, le ministère des Armées a commencé sans tarder sa transformation numérique (TN). Elle est marquée par des documents fondateurs qui reflètent autant les ambitions que la définition des priorités et la structuration de ces ambitions. La prise en compte des nombreuses spécificités des armées s'est avérée un préalable essentiel de cette démarche. En effet, le ministère se distingue par une grande diversité de métiers, avec des femmes et des hommes en opérations sur terre, dans les airs, sur et sous les mers. Il s'agit également d'hôtellerie, de l'exploitation de réacteurs nucléaires, d'habillement, des hôpitaux, des pompiers, des infrastructures, des satellites, etc. Le système d'information est structurant : un réseau interne de 220 000 machines, des réseaux classifiés, plus de 10 000 postes de travail, 1 600 systèmes d'information exploités, plus de 1 000 sites en France métropolitaine, outre-mer et dans le monde. En outre, le ministère opère son propre système de communication par satellite ou liaisons radio de toutes gammes.

La ministre des Armées, Florence Parly, a lancé en septembre 2017 la démarche de transformation numérique. Celle-ci a une résonance particulière pour les armées, confrontées à une course à la supériorité opérationnelle passant par la maîtrise du numérique. Les enjeux de souveraineté et de sécurité en sont des prérequis indispensables.

Les armées, précurseurs étatiques de la transformation numérique

Une inscription de la transformation dans celle de l'État

Le rôle des armées dans la cyberdéfense a été présenté dès le *Livre blanc* de 2008, puis confirmé avec de nouvelles ambitions dans celui de 2013. Le Premier ministre Manuel Valls a ensuite défini les objectifs de la stratégie nationale pour la sécurité du numérique en 2015, le ministre de la Défense Jean-Yves Le Drian a créé un

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

commandement Cyber (Comcyber) en décembre 2016, soulignant que « l'arme cyber est une arme à part entière, qui fait partie des moyens à disposition du commandement militaire ». Le fait « cyber » a désormais toute sa place dans la politique de défense de la France. La réflexion engagée sur le cyberespace s'est poursuivie par une prise en compte des évolutions nécessaires de la dimension numérique du ministère des Armées. L'approche initiale technique a ainsi été prolongée par une approche globale des enjeux de la révolution numérique. À ce titre, la dimension numérique est présente tout au long de la *Revue stratégique de défense et de sécurité nationale* présentée en octobre 2017 au président de la République.

> La révolution numérique sera un vecteur fort de cette transformation. Je veux la mettre au service du ministère : l'Internet des objets, l'intelligence artificielle ou le big data sont autant de chantiers ouverts sur lesquels nous devons appuyer le succès de nos armes, l'efficacité et l'excellence dans la conduite de toutes les missions du ministère.
>
> Mme Florence Parly, ministre des Armées, *Ambition numérique*, novembre 2017.

La vision globale de la transformation numérique du ministère des Armées a été définie dans le document *Ambition numérique* (novembre 2017) qui fixe trois objectifs stratégiques : garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations ; renforcer l'efficience des soutiens et faciliter le quotidien des personnels ; améliorer la relation au citoyen et l'attractivité du ministère. L'ambition de transformation contribue à renforcer le dynamisme et la modernité des armées. C'est une démarche volontaire visant à s'approprier au plus vite et dans les meilleures conditions les technologies émergentes, pour provoquer des ruptures dans les usages et les modes de travail, et, *in fine*, mieux remplir les missions dévolues au ministère. Les quatre feuilles de route de ce chantier numérique couvrent la gouvernance et les nouveaux processus pour aller vers plus d'agilité et de meilleurs contrôles financiers, les technologies numériques – dont la migration vers le *cloud*, et les données cartographiées et ouvertes pour en assurer une meilleure exploitation – et, enfin, les ressources humaines avec la volonté d'accroître le niveau d'acculturation au numérique du personnel et de mieux former et fidéliser ses spécialistes. Elles sont déclinées ci-après.

L'inscription de la transformation numérique du ministère dans la Loi de programmation militaire (LPM) 2019-2025 conforte le dynamisme et la modernité du ministère des Armées, en lui octroyant les moyens de concrétiser cette ambition, à l'image des 1 500 postes supplémentaires qui seront ouverts d'ici 2025 dans le domaine de la cyberdéfense et de l'action numérique. Cet effort en matière de ressources humaines s'accompagne d'une réflexion d'ensemble concernant le recrutement, la formation/acculturation au numérique et la fidélisation du personnel, tant militaire que civil, en lien notamment avec la démarche « Civils de la défense » lancée par la ministre.

La transformation de la DGSIC en DGNUM

La création du Comcyber, puis de la DGNUM dans le courant de l'année 2018 démontre que le ministère a adapté son organisation pour répondre aux défis posés par l'espace numérique, milieu évolutif, compressé et fait d'immédiateté, qui interroge l'ensemble de nos modèles.

> Ainsi, j'ai voulu une DGNUM chef d'orchestre, dotée d'instruments adaptés à sa mission de transformation. En appui des armées, directions et services, elle veille au pilotage des projets numériques, elle promeut de nouveaux modes de management et de développement plus agiles, mieux sécurisés, plus flexibles.
>
> Discours de Mme Florence Parly, ministre des Armées, « Un an de transformation numérique », Paris, 7 février 2019.

Précurseur parmi les autres administrations, le ministère des Armées s'est doté en avril 2018, du *Plan de transformation numérique-Défense Connect*, et a créé, en juin 2018, la Direction générale du numérique et des systèmes d'information et de communication (DGNUM), en remplacement de la DGSIC. Directement rattachée à la ministre des Armées, elle a pour mission d'orchestrer la TN au sein du ministère et d'assurer une gouvernance globale garantissant la cohérence d'ensemble des systèmes d'information et de communication (SIC). L'administration ministérielle des données est également de son ressort.

La TN n'est pas évidente mais est inéluctable. Il s'agit d'un changement majeur de culture qui s'accompagne de besoins nouveaux, en termes de ressources humaines notamment. La DGNUM est responsable de la modernisation du système d'information et de communication, et agit ainsi en véritable direction des systèmes d'information de groupe. Elle contrôle l'application de la politique ministérielle et coordonne l'ensemble des structures et ressources du ministère en matière de SIC. Elle élabore la politique générale en matière d'utilisation du spectre de fréquences du ministère et veille à la coordination des besoins en fréquences des utilisateurs du ministère. Désormais dotée d'outils d'encadrement de la transformation numérique, la DGNUM contrôle l'application des décisions et directives. Elle veille également à être toujours en symbiose avec les métiers placés sous la responsabilité des grands subordonnés du ministre : le chef d'état-major des armées (CEMA), le secrétaire général pour l'administration (SGA) et le délégué général pour l'armement (DGA).

Enfin, la DGNUM est administrateur ministériel des données et pilote des métiers du numérique. Les enjeux des politiques de transformation numérique sont majeurs en termes de souveraineté nationale.

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

La souveraineté capacitaire : théorie et pratique dans les armées

L'exercice de la souveraineté se traduit par une stratégie qui s'intègre efficacement dans le déploiement de la politique numérique de l'État. La souveraineté numérique, c'est-à-dire l'autonomie stratégique dans le domaine numérique, doit pouvoir être garantie par une capacité d'action. L'autonomie nécessaire à la souveraineté ne doit pas être confondue avec une indépendance ou une autonomie totale des moyens. Les armées n'ont pas la possibilité de contrôler de bout en bout l'autonomie de leur production en électronique et en informatique. Le recours à des éléments produits par des entreprises privées et/ou étrangères est inévitable et comporte un risque intrinsèque. Partageant, sur ce point-là, la position d'autres partenaires, la France a fait le choix de prioriser la sécurisation des moyens vitaux. Les armées n'ont ainsi besoin de maîtriser que certains composants bien précis pour pouvoir sécuriser un ensemble composé de briques. Cette démarche repose tout d'abord sur le développement et la mise en œuvre d'outils de cryptographie souverains pour assurer l'intégrité et la confidentialité des données. Ensuite, la maîtrise des réseaux passe par la possession de sondes de détection entièrement fiables et maîtrisées, afin de garantir la disponibilité des données. Enfin, il faut des algorithmes nationaux pour assurer le traitement de ces données.

L'absence de confiance totale dans les matériels et logiciels utilisés est palliée par le chiffrement et l'assurance de la disponibilité du service grâce aux outils de détection. Les armées ne sont pas pleinement autonomes en matériels et en logiciels mais elles assurent une forme d'indépendance par la diversité des sources d'approvisionnements et de fabrications, et l'emploi de plusieurs réseaux protégés et physiquement séparés. En outre, croire que les composants ou les logiciels pourraient tous être nationaux ou européens est une illusion. Cet effort serait inutile car, même développés en propre, les produits numériques ne pourront jamais être considérés comme parfaitement fiables. De plus, leur maintien à jour et en conditions de sécurité est bien souvent un défi coûteux, rendant les logiciels propriétaires non nationaux très attractifs.

La feuille de route « Gouvernance, pilotage et conduite de projets »

Les transformations inhérentes à la feuille de route « Gouvernance, pilotage et conduite de projets » reposent notamment sur l'introduction de nouveaux modes de conduite des projets, à l'instar de la méthode Agile. Ces solutions plus flexibles, tout en maintenant le niveau de sécurité attendu, permettent d'être adaptées au rythme rapide des évolutions numériques.

Une refonte de la méthodologie des projets

La supériorité opérationnelle passe notamment par l'intégration et l'utilisation des solutions numériques et par des modes de développement agiles qui produisent des services numériques plus rapidement qu'avec la procédure conventionnelle. Plusieurs éléments freinent leur mise en place : des difficultés d'industrialisation des *Proof of Concept* (POC) ainsi qu'une difficulté à intégrer les solutions numériques aux services existants. Deux grands objectifs se dégagent de ce constat. Le premier concerne la politique et la gouvernance de l'innovation numérique : il faut créer les conditions d'émergence et de mise en œuvre de ces innovations. Le deuxième concerne le processus global d'innovation numérique : il est nécessaire de définir un processus continu, de l'idéation à la mise en service.

Défense Connect*, un levier fondamental de la transformation*

La création de la marque *Défense Connect*, sous laquelle l'ensemble des projets liés à la transformation numérique du ministère est fédéré, confère une cohérence ministérielle. Cette initiative offre une compréhension plus fine et une meilleure identification d'un processus de transformation numérique d'ampleur au service de la modernisation du ministère des Armées, ainsi qu'une vision transverse aux usagers civils et militaires de la création d'une offre de nouveaux services visant à renforcer l'efficacité des soutiens et le quotidien du personnel.

D'un point de vue institutionnel, *Défense Connect* adosse symboliquement le ministère des Armées à la démarche interministérielle *Tech. Gov*, portée par le Premier ministre et la DINSIC devenue DINUM. *Tech. Gov* recouvre, d'une part, une solution technique unique d'identification sécurisée sur l'Internet et, d'autre part, l'ambition gouvernementale de transformation numérique portée par la démarche *Action publique 2022*. Dans cette logique, le rayonnement interministériel de *Défense Connect* favorise la lisibilité de l'action du ministère des Armées, soulignant sa contribution et sa forte implication dans la réussite de ce chantier global.

Défense Connect facilite enfin la visibilité de nos actions en direction de notre écosystème (écoles, incubateurs, groupements, entreprises, PME, start-up), et favorise la visibilité du ministère en tant qu'acteur majeur du numérique et administration engagée dans une démarche d'excellence et d'expertise. *In fine*, *Défense Connect* contribue à l'attractivité du ministère, dans un domaine où les ressources humaines sont fortement contraintes et les hauts potentiels disputés au secteur privé.

La création de la marque *Défense Connect* remplit ainsi sept objectifs essentiels :

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

1. Soutenir les partenariats au niveau national et promouvoir les acteurs de l'écosystème numérique en France : le ministère des Armées a été le premier des ministères français à publier son schéma directeur et est pris en exemple au plan interministériel. Il occupe une place centrale dans les réflexions touchant au numérique (souveraineté numérique, utilisation des données, stratégie industrielle, etc.). Les questions de TN et de SIC font aujourd'hui l'objet de différentes coopérations interministérielles.

2. Soutenir, faire connaître et valoriser les actions de transformation et les innovations numériques réalisées par le ministère au service de sa modernisation : *Défense Connect* contribue à montrer que la TN est inéluctable et constitue une composante indispensable de la condition des forces et du succès des opérations.

3. Développer l'acculturation et les compétences numériques : la structuration d'une offre de formation *Défense Connect* adaptée à tous les niveaux de responsabilité des agents dans le domaine du numérique est en cours.

4. Développer une image de marque et d'employeur pour la TN, favorisant l'attractivité du ministère : cela passe par la promotion de la diversité des métiers et des parcours du numérique au sein du ministère pour attirer les talents. Cet objectif va de pair avec une volonté de réduire les inégalités vis-à-vis de certains segments de population (femmes, personnes en situation de handicap, etc.).

5. Fédérer les acteurs de la TN (militaires, civils, réservistes) autour d'une identité commune : il s'agit notamment de favoriser un esprit d'équipe numérique contribuant à enraciner la TN au sein du ministère par la fidélisation de ses acteurs au sein de la filière SIC-Numérique.

6. Mettre le ministère dans une logique de plateforme, à l'instar des sociétés qui ont passé le virage du numérique.

7. Donner les moyens, par la Fabrique numérique, de délivrer rapidement et efficacement les services numériques.

La feuille de route « Technologie »

La feuille de route « Technologie » est orientée sur la simplification du SI ministériel et son adaptation aux nouveaux usages numériques mais également aux besoins des utilisateurs et des métiers. A ainsi été créée l'Unité de management Socle numérique (UM SNUM), unité mixte entre la Direction générale de l'armement (DGA) et la Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense (DIRISI). Les travaux de l'UM SNUM permettent de garantir la cohérence d'ensemble et de faciliter la continuité entre les activités de conception et de développement (DGA), d'une part, et les activités de déploiement et d'exploitation d'autre part (DIRISI). L'hébergement sécurisé

et le développement du *cloud*, la confiance et la sécurité numériques, la mise en œuvre de technologies de rupture (IA, *big data*, etc.) font également l'objet d'études approfondies. La liste n'est pas exhaustive. Enfin, le ministère possède un important *legacy* représenté par les systèmes en service et qui est, pour partie, obsolète. Il représente une lourde dette technologique et sécuritaire et un enjeu de rattrapage numérique important.

La création de l'UM SNUM

La création de l'UM SNUM découle du constat de la nécessaire prise en compte des nouvelles technologies dans l'ambition numérique du ministère. La capacité de traitement massif d'informations ainsi que le besoin d'une plus grande adaptation au monde ouvert de l'Internet ont notamment été mis en avant. Les différentes réflexions conduites ont permis d'aboutir au besoin de construire un outil de travail, dont la mission est de fournir des services relatifs au socle numérique du ministère.

L'UM SNUM contribue intrinsèquement à opérer une rupture essentielle : faire passer le ministère des Armées d'une « logique projet » à une « logique produit/service ». Cette création accompagne la réorganisation du paysage SIC avec la redéfinition du périmètre de chacun des acteurs impliqués, la volonté de maîtriser le besoin d'une ressource humaine structurellement déficitaire et donc de favoriser l'intégration d'experts issus des différentes entités existantes du ministère des Armées. Ces expertises ont été mobilisées dès le second semestre 2017 pour constituer une première structure de préfiguration. En juillet 2018, la ministre a décidé la création d'une nouvelle structure dédiée, installée officiellement en juin 2019, et renforcée par un recrutement permettant d'atteindre l'objectif de 300 personnes dans les prochaines années.

La création de l'UM SNUM permet à court et moyen termes de garantir la fourniture d'un service à l'utilisateur à temps et à la demande (*time to the market*). Cette nouvelle organisation favorise également la fluidification du lien entre le socle numérique et les applications, notamment en privilégiant des processus « devops » c'est-à-dire de développement rapide. Cette évolution des processus favorise aussi le rapprochement entre l'opérateur et les applications. Cela amène une révision globale des processus de travail de la part des clients et permet un allègement du temps consacré par les agents du ministère à certaines missions ou tâches.

La centralisation du besoin et la réponse dans une « logique services » préservent le ministère de la multiplication des projets en réponse à un même besoin et permet donc de réaliser des économies d'échelle substantielles – l'offre

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

de services faite à un client peut être proposée à l'ensemble du ministère. Cette capacité de mise à disposition généralisée permettra à terme de limiter le « shadow IT », c'est-à-dire la mise en œuvre de solutions diverses à titre individuel par l'utilisateur.

La feuille de route « Données »

Ouverture maîtrisée d'un actif stratégique

Un changement de paradigme s'est produit avec l'émergence de la donnée comme capital actif du ministère et bien commun ; elle est au cœur de sa refondation numérique. Enjeu majeur, il est nécessaire d'apprendre à mieux la traiter, mieux la sécuriser au niveau national et à la partager au bénéfice de l'action globale des armées en opérations et dans le fonctionnement quotidien du ministère des Armées. Il importe de garantir que, même exportées chez des partenaires industriels à des fins de valorisation, les données resteront en toutes circonstances soumises à des règles de sécurité informatique drastiques (cybersécurité) et exposées exclusivement au régime du droit français (souveraineté numérique) et européen.

Le cadre stratégique de la gouvernance ministérielle des données est fixé dans l'instruction de la DGNUM relative à la gouvernance ministérielle des données, signée le 15 octobre 2018. Elle pose les principes directeurs applicables à l'ensemble des acteurs du ministère et définit les rôles et responsabilités de chacun, comme les fonctions des nouveaux directeurs des données. Cette gouvernance forte et transparente porte les enjeux suivants : améliorer la maîtrise du patrimoine ; connaître les données du ministère grâce à un travail de cartographie, de recensement, d'indexation et de modélisation afin de mieux maîtriser le cycle de vie des données, les gérer, les protéger et les valoriser ; faire respecter le cadre législatif, réglementaire, contractuel et éthique qui s'impose au traitement des données du ministère ; favoriser la circulation des données de référence et des données présentant un intérêt particulier pour les états-majors, directions et services du ministère ainsi que pour les industriels de défense ; favoriser l'accessibilité des données dans un format ouvert et réutilisable.

Désigné administrateur ministériel des données (AMD), la DGNUM est à ce titre responsable de la valorisation du patrimoine informationnel du ministère. Autrement dit, il doit promouvoir et maximiser les usages et innovations pouvant naître de l'exploitation des données. La DGNUM assure la mise en place d'une gouvernance ministérielle de la donnée reposant sur une double dynamique : construire en commun un cadre de confiance permettant d'ouvrir et de partager

les données de manière maîtrisée et sécurisée ; aider à construire des solutions techniques sécurisées, proposer aux métiers des offres de service en matière de cartographie, de stockage, d'exposition, d'exploitation, de partage, etc. Ce contrat de confiance est indispensable à la construction d'une organisation favorisant le partage de la donnée. Il permettra d'accompagner les acteurs spécialistes ou non, de mettre autour d'une même table producteurs et consommateurs pour traiter des modalités de mise à disposition et de consommation des données.

Par une ouverture maîtrisée de ses données, le ministère des Armées pourra gagner en réactivité, précision et fiabilité. Le partage, l'exploitation et la valorisation des données à travers les nouvelles technologies numériques permettront notamment de donner du sens aux masses de données collectées par les armées. En effet, la vision globale des situations, leur suivi en temps réel, leur anticipation, la réduction de l'incertitude dans les prises de décision, l'augmentation de la rapidité de prise de décision et l'amélioration des retours d'expérience (RETEX) sont autant de nouvelles capacités qui pourront être fournies aux armées par le partage et l'exploitation des données couplées à l'utilisation des technologies numériques.

Alors que le niveau de maturité du ministère sur cette question est variable et globalement assez faible, l'ouverture maîtrisée des données et leur partage demande trois capacités fortes, indispensables pour une exploitation optimale d'outils de type *big data* et IA : une gouvernance ministérielle volontariste, fondée sur une culture de confiance et de partage maîtrisé, seule capable de dépasser les silos – cette démarche sera applicable tant au sein du ministère qu'en direction de nos partenaires industriels de défense ; la capacité à attirer les compétences et à acculturer les agents pour faire de la donnée un outil du quotidien ; la capacité à stocker, valoriser et mettre à disposition des données de qualité au profit du *big data* et de l'IA *via* des technologies comme le *cloud*, avec le concours de partenaires respectueux et soucieux de notre autonomie stratégique et des enjeux de souveraineté.

Hébergement d'un bien commun national

Pour la période post-2020, dans le cadre de la doctrine d'utilisation de l'informatique en nuage par l'État, la ministre des Armées a mandaté la DGNUM pour conduire l'étude, l'orientation et la définition d'une feuille de route sur les nouvelles solutions d'hébergement accessibles aux usagers du ministère et pour proposer la stratégie industrielle associée. Cette démarche a notamment pour vocation de permettre l'exploitation massive des données qui recouvre nombre de potentialités dans les domaines des opérations (réduction de l'incertitude, supériorité informationnelle, fusion du renseignement, etc.), du soutien (la maintenance dite cognitive,

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

tenant compte du contexte et des conditions d'emploi des systèmes) et du service rendu à l'usager. L'ouverture des données au sein d'une organisation impose un changement de culture, tant dans l'organisation que dans les usages, et un nécessaire choix de solutions techniques spécifiques pour stocker et partager les données.

La migration de tout ou partie des systèmes d'information sur une architecture type *cloud* est envisagée à moyen terme. Cette évolution sera la seule à même de garantir le passage à l'échelle des capacités de stockage et de traitement massif des données, industrialisant le recours à de nouvelles technologies comme l'IA et le *big data*. Le ministère examine la possibilité de concilier un « *cloud* privé » physiquement localisé dans ses emprises, et un « *cloud* dédié » situé chez des partenaires respectueux et soucieux de l'autonomie stratégique des armées et des enjeux de souveraineté. La première option permettra l'hébergement des systèmes essentiels aux opérations militaires et des systèmes traitant de données confidentielles. Il devra apporter au ministère des Armées une maîtrise complète de la sécurité et de la résilience en situation de crise extrême pour la nation. La seconde aura pour vocation d'héberger la majorité des systèmes du ministère et de servir de zone d'échange pour les données sensibles du ministère, étant précisé que le volet cyber ne sera pas délégué. En effet, la donnée constitue un bien commun national qu'il convient de préserver et de protéger. Ce « *cloud* dédié » ne pourra être confié qu'à des partenaires de confiance, partageant une même « communauté de destin ». Il permettra en outre au ministère des Armées de bénéficier de la valeur ajoutée proposée par les partenaires fournisseurs de *cloud*, et donc de services performants, sécurisés et actualisés.

Promouvoir la culture de valorisation des données, accroître la « datalphabétisation » des agents, faire du ministère des Armées un ministère *data-driven*, utiliser les nouvelles technologies et les innovations numériques comme levier de performance, explorer toutes les applications opérationnelles et concrètes du *big data* et de l'IA figurent parmi les nombreux chantiers de la transformation numérique.

La feuille de route « Ressources humaines »

La feuille de route « Ressources humaines » repose sur la capacité du ministère des Armées à recruter et gérer les compétences numériques indispensables à sa transformation dans des domaines de niche ou autrefois inexistants, tout en assurant la pérennité de sa filière SIC et l'acculturation des agents déjà présents au sein de l'institution. Le numérique entraînant une accélération de l'évolution des métiers et des compétences, il apparaît indispensable que l'ensemble du personnel du ministère soit accompagné dans la TN. Le défi est notamment de permettre à chacun de s'approprier le numérique et ses enjeux.

La Direction des ressources humaines du ministère (DRH-MD) et la DGNUM travaillent à une réforme de la filière SIC pour la revaloriser et la rendre plus attractive. Le développement et l'enrichissement progressif de l'offre de formation s'adossent à la mise à disposition des agents d'outils d'acculturation comme le Passeport numérique.

Depuis 2018, un Passeport numérique est mis à disposition des agents civils et militaires sur l'intranet du ministère. Composé d'activités interactives, de vidéos et de questionnaires, il offre à chacun un socle de connaissances minimal sur le numérique, ses enjeux notamment de sécurité, et ses implications dans le milieu professionnel. Il sera complété par la création d'une Académie du numérique pour le développement d'une offre de formation auprès de nombreux partenaires et adaptée à la multiplicité des profils académiques et professionnels des agents.

Des réseaux comme le Cercle *Défense Connect* ou encore le réseau Combattantes@Numérique ont également été mis en place.

Le Cercle *Défense Connect* est un espace de réflexion sur les questions liées au numérique. Placé sous le patronage du chef d'état-major des armées (CEMA), il est constitué de responsables de l'écosystème civil et des plus hauts responsables du ministère. Il inclut 13 entreprises françaises partenaires et des représentants du monde académique. Les travaux du Cercle ont un double objectif. Il s'agit de renforcer la coopération entre des organismes privés et le ministère des Armées d'une part et, d'autre part, de permettre l'acculturation des 30 plus hauts responsables du ministère sur les sujets de transformation numérique. La DGNUM s'implique aussi dans le Cigref pour des opérations de conseils et des mesures d'accompagnement.

Enfin, le réseau Combattantes@Numérique, inspiré de l'initiative nationale Femmes@Numérique, est né en septembre 2018 sur l'impulsion de la DGNUM. Il est composé de plusieurs dizaines de femmes issues des filières numériques du ministère des Armées avec une représentation homogène de statuts (militaires, civils), classes d'âge, filières et grades. Il vise à encourager les femmes à s'approprier les compétences numériques, contribuant ainsi à l'anticipation des besoins des métiers du numérique et de la société de demain.

Conclusion

Le ministère des Armées a ainsi engagé sa transformation numérique, lancée par la ministre Florence Parly dès septembre 2017 et orchestrée par la nouvelle Direction générale du numérique. Cette transformation vise, au travers de nouveaux usages, à s'approprier rapidement et dans les meilleures conditions les technologies émergentes, pour engager des ruptures dans les pratiques, les organisations et les modes de travail ou d'action. Elle implique un véritable changement de

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

culture à tous les niveaux du ministère, pour mettre la donnée au cœur de ses opérations, de ses équipements et de son administration. Cela nécessite de développer des capacités pour apprendre à mieux traiter la donnée, la sécuriser au niveau national, la stocker à travers le *cloud* notamment et la partager au bénéfice de l'action globale des armées. Alors que l'espace numérique est devenu un enjeu stratégique majeur, cette transformation numérique est la condition de notre autonomie stratégique, gage de l'exercice de la souveraineté nationale.

Bibliographie

Arrêté du 28 juin 2018 portant organisation de la direction générale du numérique et des systèmes d'information et de communication, *JORF*, n° 0148 du 29 juin 2018, texte n° 14.

Arrêté du 28 juin 2018 modifiant l'arrêté du 31 décembre 2003 relatif au conseil de gestion de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense, *JORF*, n° 0148 du 29 juin 2018, texte n° 15.

Arrêté du 28 juin 2018 pris pour l'application de l'article 5 du décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication, *JORF*, n° 0148 du 29 juin 2018, texte n° 16.

CABINET DE LA MINISTRE DES ARMÉES (2019), Instruction n° 100 relative aux opérations d'investissement du ministère des Armées, 15 février 2019.

– Instruction n° 2476/ARM/CAB/CC6 portant sur la conduite des projets de système d'information et de communication, 29 avril 2019.

Décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication, *JORF*, n° 0148 du 29 juin 2018, texte n° 13.

MINISTÈRE DE LA DÉFENSE (2008), *Défense et sécurité nationale. Livre blanc*, Odile Jacob/ La Documentation française, Paris.

– (2013), *Livre blanc. Défense et sécurité nationale*, Paris.

MINISTÈRE DES ARMÉES (2017), « Ambition numérique », 30 novembre.

– (2018), note n° 409 du 8 octobre 2018 portant sur la conduite agile des services digitaux.

– (2018), Instruction ministérielle n° 2 du 15 octobre 2018 portant sur la gouvernance ministérielle des données.

– (2019), note n° 44 du 11 février 2019 portant sur la politique générale sur le logiciel au ministère des armées.

– (2019), « Un an de transformation numérique », Discours de Mme Florence Parly, Ministre des Armées, Paris, 7 février 2019.

PRÉSIDENCE DE LA RÉPUBLIQUE (2017), *Revue stratégique de défense et de sécurité nationale*, Paris.