

## 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>  
-----

Distribution électronique Cairn.info pour La Découverte.

© La Découverte. Tous droits réservés pour tous pays.

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur en France. Il est précisé que son stockage dans une base de données est également interdit.

# La transformation numérique du ministère des Armées

Arnaud Coustillière<sup>1</sup>

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'efficacité 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

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 cyberspace 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'efficacité 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.

*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 :

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 de *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

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,

tenant compte du contexte et des conditions d'emploi des systèmes) et du service rendu à l'utilisateur. 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 « dataphabétisation » 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 inexistantes, 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'adosent 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

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