



CONCOURS INTERNES SUR ÉPREUVES DE RECRUTEMENT DE COMMISSAIRES DES ARMÉES EN 2022

RÉDACTION D'UNE NOTE ADMINISTRATIVE

durée : 4 heures

Concours au titre du 2° de l'article 4 du décret n°2012-1029 du 5 septembre 2012 : coefficient 5

Concours au titre du 2° de l'article 6 du décret n°2012-1029 du 5 septembre 2012 : coefficient 10

« La transformation numérique des armées »

Le Ministère des armées n'échappe pas à la dynamique de transformation numérique en œuvre au sein de la fonction publique, et plus largement dans l'ensemble de la société française. Pour autant, les enjeux de cette transformation sont nombreux et souvent très spécifiques au sein des armées.

Vous êtes affecté à la direction centrale du service du commissariat des armées et votre chef de service, chef de la Division numérique, vous demande de rédiger une note administrative dans la perspective de sa participation à un séminaire organisé par l'Etat-major des armées sur la stratégie numérique des armées. Cette note synthétisera les principaux enjeux liés aux dynamiques actuelles de la digitalisation au sein des armées, en n'omettant pas d'apporter un éclairage particulier sur les enjeux propres à l'administration et aux soutiens.

A l'aide des documents joints vous rédigerez ainsi une note synthétisant cette question et faisant apparaître des propositions d'actions à même de permettre cette transformation.

Ce travail ne doit pas dépasser **quatre pages manuscrites de synthèse et une page manuscrite de propositions d'actions concrètes à mener à court terme.**

SOMMAIRE

Pièce	Titre	Référence
1	<i>Armées 4.0 : il est urgent que la France se lance dans la bataille !</i>	www.latribune.fr – 13 avril 2021
2	<i>Révolution numérique : vers une armée numérique ?</i>	www.geostrategia.fr – 27 mars 2018
3	<i>Le numérique, au cœur des priorités du SCA</i>	portail-commissariat.intradef.gouv.fr
4	<i>Qu'est-ce que la transformation numérique ?</i>	portail-transformation-numerique.intradef.gouv.fr
5	<i>Optimiser l'exploitation des données dans le secteur public</i>	www.bearingpoint.com
6	<i>Secteur public : comment automatiser les processus mais pas leurs complexités ?</i>	www.hubinstitute.com – 2 mars 2020
7	<i>SIRH 2022 : une feuille de route en 6 axes pour la transformation numérique de la fonction RH</i>	www.fonction-publique.gouv.fr

Document 1 : « Armées 4.0 : il est urgent que la France se lance dans la bataille ! » - www.latribune.fr – 13 avril 2021

« Armée 4.0 » : il est urgent que la France se lance dans la bataille !

OPINION. L'armée française doit opérer une mue numérique nécessaire, à l'aune des nouvelles menaces technologiques qui émergent chaque jour et la mutation des conflits auxquels l'État fait face. (*) Par Christophe Négrier, vice président Oracle Technology

Christophe Négrier (*)

13 Avr 2021, 8:00

Les conflits que nous avons connus tout au long du XXe siècle ne seront probablement pas ceux que nos enfants connaîtront demain. Les grandes révolutions numériques bouleversent en profondeur la nature des menaces auxquelles sont confrontés les États. Cyberspace, drones autonomes, reconnaissance faciale...La guerre des données et la robotisation auront un rôle croissant et central dans l'arsenal militaire des grandes puissances mondiales.

Avec un budget de 750 millions d'euros en R&D chaque année, la France est le premier investisseur étatique européen dans le secteur de la défense. Ces investissements permettent à nos armées (Terre, Mer, Air et Gendarmerie) de développer des outils innovants, capables de répondre aux nouvelles menaces. Ainsi, le numérique à travers les technologies d'Intelligence Artificielle (IA), de Machine Learning et du Big Data sont devenus indispensables sur les différents terrains d'opérations à travers le monde.

1.1. Une mue numérique nécessaire et hautement stratégique

Si la science-fiction illustre régulièrement ce que sera, ou pourrait être, l'armée du futur, la défense a aujourd'hui un enjeu bien plus réaliste à court terme : le maintien en condition opérationnelle (MCO) de son matériel, c'est-à-dire la modernisation de l'ensemble des moyens humains, techniques et financiers au service des armées - en France et sur les théâtres extérieurs. Le MCO est un rouage essentiel de la stratégie de modernisation du ministère des Armées, tant par son impact opérationnel, le moindre retard pouvant nuire aux forces déployées, que les coûts qu'il entraîne.

La mue technologique de l'armée, et la migration vers des solutions plus performantes et moins coûteuses permettent d'optimiser les ressources humaines, et les dépenses d'infrastructure qui pèsent sur le budget annuel du ministère des Armées. C'est en s'inspirant du modèle de "l'industrie 4.0" et de ses outils technologiques que les armées pourront se transformer efficacement.

1.2. Big data et intelligence artificielle, des alliés de choix

Si le Big Data a révolutionné de nombreux usages, il s'est également frayé un chemin au sein des forces armées et de leurs instances décisionnaires. Géolocalisation, systèmes d'armement, gestion du trafic aérien ou maritime... L'activité militaire s'est profondément numérisée et génère chaque jour une quantité croissante de données. Au même titre que l'industrie ou les administrations, l'armée doit désormais apprendre à tirer pleinement parti de ses données.

Annoncée comme l'une des priorités de la ministre des Armées Florence Parly en 2019, l'IA est devenue un atout essentiel des forces militaires. Nourrie par les données agrégées sur le terrain, elle est la clé d'une meilleure compréhension de certaines situations, d'une meilleure capacité décisionnelle, mais aussi d'une automatisation des opérations courantes. Si les pistes d'application sont nombreuses, l'IA montre déjà son utilité pour la sécurité intérieure. A travers un algorithme, elle trie automatiquement les données collectées sur internet, et offre une capacité d'analyse sémantique pour détecter des signaux - même faibles - de radicalisation sur les réseaux sociaux, par exemple.

Elle est également très utile pour le contrôle des frontières, l'analyse des arrivées-sorties du territoire, et le croisement avec des fichiers d'individus recherchés. Même si la France n'envisage pas de construire des systèmes pleinement autonomes, l'IA reste un outil d'aide à la décision pour les opérations extérieures, notamment pour gérer la détection et l'anticipation des menaces.

1.3. La 5G et l'IoT, prochains bras armés de la France ?

La 5G sera indéniablement une source d'amélioration de la vie des citoyens. Mais pas seulement. Elle ouvre également la voie à une nouvelle étape dans la transformation numérique de nos armées et de leurs outils. Technologie fiable, performante et ultra rapide, elle permet aujourd'hui le déploiement de réseaux privés, indispensables à une gestion optimisée des opérations militaires.

Associé à un Cloud sécurisé, un réseau 5G privé réduit ainsi la latence des communications et facilite l'utilisation de vidéos et capteurs sur les différentes zones de combat, en lien avec le poste de commandement, le groupement tactique et les points de débarquement aériens. En parallèle, elle permet d'améliorer la sécurité des convois logistiques, régulièrement utilisés pour les ravitaillements terrestres - mais trop souvent la cible d'attaques armées. Grâce à la 5G équipant les véhicules militaires, les convois pourront à terme circuler de façon entièrement autonome, le long d'un itinéraire sécurisé.

Enfin, s'il est encore trop tôt pour parler de soldat augmenté, l'Internet des Objets (IoT) offre des ressources précieuses, notamment pour le suivi en temps réel de la santé des troupes. Le déploiement de capteurs permettrait ainsi de suivre l'état de chaque soldat pour assurer une prise en charge rapide et adaptée en cas de blessure, ainsi qu'un service de téléconsultation depuis le théâtre d'opération.

1.4. A quand un cloud de défense pour la France ?

Si nous sommes encore loin de l'armée futuriste que décrivent certaines œuvres littéraires d'anticipation, la défense a tout de même entamé sa mue technologique. Mais ce mouvement ne doit pas être autarcique - une mutualisation internationale des dépenses, et des investissements est possible aussi bien au niveau de l'Union européenne, que de l'OTAN. Fin janvier, l'Alliance transatlantique a choisi son partenaire technologique pour équiper son futur cloud de défense visant à développer des communications ultra-sécurisées entre son centre de commandement et ses théâtres d'opérations, et ainsi faciliter l'interopérabilité entre ses membres.

Il est temps pour la France de saisir à son tour cette occasion de se lancer dans la bataille et d'accentuer ses propres investissements pour faire face aux nouvelles menaces technologiques. Pour les années à venir ; mais dès que possible.

Christophe Négrier (*)

Document 2 : « Révolution numérique : vers une armée numérique ? » - www.geostrategia.fr – 27 mars 2018



Révolution numérique : vers une armée numérique ?

Erwan Rolland

La problématique de l'adaptation de notre outil de défense aux défis posés par la révolution numérique anime et structure la réflexion de l'auteur de cet article. Cette révolution, par sa nature et par son ampleur, ouvre un nouvel espace de confrontation qui requiert une profonde réorganisation. Cette réorganisation pourrait prendre différentes formes et l'auteur propose plusieurs scénarii pour une « armée numérique » qui devra relever un double défi, en faisant converger efficacité opérationnelle et maîtrise de la ressource humaine.

Les opinions exprimés dans cet article n'engagent pas le CSFRS.

Les références originales de ce texte sont Erwan Rolland « Révolution numérique : vers une armée numérique ? »

Ce texte, ainsi que d'autres publications peuvent être visionnés sur le site du [CHEM](http://www.dems.defense.gouv.fr/chem/)
: www.dems.defense.gouv.fr/chem/

Révolution numérique : vers une armée numérique ?

L'organisation actuelle de notre outil de défense ne doit pas être un frein aux potentialités que laissent entrevoir la révolution numérique, les technologies émergentes et les ruptures qu'elles préfigurent. La croissance rapide des technologies de l'information et de la communication et l'innovation dans les systèmes numériques nécessitent de se poser la question sur la pertinence de bâtir dès à présent un modèle d'armée numérique capable de répondre aux défis opérationnels à venir à horizon 2030.

Sur la base d'un état probable de maturité de ces nouvelles technologies et des menaces qu'elles feront (et font déjà) peser sur nous, cette étude se propose de jeter les prémices des contours que pourraient prendre une véritable armée numérique.

L'enjeu pour la France et ses armées est de disposer d'une organisation dédiée lui permettant d'assurer sa défense et sa sécurité en optimisant l'emploi et les potentialités

numériques du cyberspace, en parfaite complémentarité avec les forces conventionnelles des autres milieux.

Une révolution numérique en marche

Une révolution numérique encore en devenir

La croissance rapide des nouvelles technologies de l'information et de la communication (NTIC) et l'innovation dans les systèmes numériques sont à l'origine d'une révolution qui ouvre de nouvelles perspectives à la création du savoir et la diffusion de l'information et qui bouleverse radicalement nos modes de pensée, de comportement, de communication et de travail. Cette *révolution numérique*^[1] peut ainsi se résumer par l'essor récent de l'informatique et de l'Internet et des mutations profondes qui se traduisent par une mise en réseau planétaire des individus, de nouvelles formes de communication (courriels, réseaux sociaux), une décentralisation dans la circulation des idées et de nouveaux modes de création de valeur et d'activités économiques.

Cette révolution numérique se caractérise par une véritable *déferlante digitale* qui, depuis l'apparition d'Internet dans les années 90 et de l'*iPhone* en 2007, a fait surgir autant de nouveaux usages que de nouveaux acteurs imprévus (GAFAM : Google, Apple, Facebook, Amazon, Microsoft...) et plus agiles que *l'establishment* économique et institutionnel. Si la révolution numérique semble remettre fondamentalement en cause les règles actuelles du jeu économique, elle rend aussi plus flou un avenir encore mal cerné. Pour beaucoup d'acteurs économiques et institutionnels (défense, sécurité, éducation, formation professionnelle, administrations...) le mot d'ordre est donc de s'adapter rapidement avant d'être dépassé et disparaître.

Cette révolution numérique à tout va se caractérise aussi par la dématérialisation (dont la démonétisation), la *désintermédiation* (ou *ubérisation*) et donc la disruption en perturbant le jeu des acteurs en place, les modes de vie et de fonctionnement qu'elle remplace ou élimine. Elle altère la structure et la nature même des différents secteurs d'activités économiques et étatiques régaliens et expose de ce fait les grands acteurs à la fois à de nouvelles menaces mais aussi de fabuleuses opportunités.

Puisque le numérique rend perméable toutes les frontières, ses succès et ses contradictions touchent aussi bien la dimension internationale que le niveau le plus micro de la société et de la politique, dont les questions de sécurité et de défense^[2]

Les perspectives d'un futur *supercalculateur quantique* pouvant casser tous les systèmes de cryptage ou d'imprimantes 3D permettant à des groupes terroristes de réaliser des armes par *fabrication additive*^[3] obligent les acteurs de la défense et de la sécurité nationale à conserver un temps d'avance et à évaluer les menaces possibles du futur pour mieux s'y préparer.

La défense et la sécurité ne sont bien évidemment pas épargnées

Si l'on s'appuie à la fois sur la loi de Moore^[4] (qui a trait à l'évolution exponentielle de la puissance de calcul des ordinateurs) et sur la convergence des grandes révolutions technologiques à venir, l'impact potentiel sur l'ensemble de nos activités et plus encore sur les questions de sécurité et de défense est considérable. L'apparition de modes d'action novateurs permettant une atténuation de l'asymétrie des conflits peut en effet avoir un effet disruptif conduisant à l'émergence de nouvelles stratégies de défense, de nouveaux modèles d'organisation militaire et de conduite des opérations.

La convergence inéluctable des domaines relevant des Nanotechnologies, Biotechnologies, de l'Informatique et des sciences Cognitives (NBIC) ouvriront très certainement la voie vers l'homme augmenté et seront également source de risques et d'opportunités dans le domaine militaire. Des exemples tirés de l'actualité récente témoignent des grandes ruptures technologiques à venir et de leur impact immédiat sur les questions de sécurité et de défense.

Les drones, la robotisation et l'intelligence artificielle (IA). En janvier 2017^[5], le Pentagone annonçait avoir testé avec succès un essaim d'une centaine de petits drones. Les progrès de l'IA rendent désormais possible la constitution de groupes de petits robots agissant collectivement pour remplir des missions coordonnées. Si certains drones sont détruits, l'ensemble continue à agir en se réorganisant. Lors de cet essai, les drones ont démontré qu'ils parvenaient à prendre des décisions collectives, adaptant ainsi leur comportement individuel aux aléas de la mission. Dessinés pour voler au moins par groupe de 20 ou plus, avec une mission bien définie à réaliser, les drones forment un organisme collectif, partageant un cerveau commun. Parce que chaque drone communique et collabore avec chacun de ses homologues, l'essaim n'a pas de leader et peut s'adapter au fur et à mesure si un nouveau drone rejoint le groupe ou si au contraire un drone est abattu.

Ces essaims de drones, peu coûteux à fabriquer et tirant leur force de leur capacité à submerger par leur nombre les défenses de l'adversaire sont très certainement amenés à avoir un bel avenir et illustrent parfaitement ce que les armées sont en droit d'attendre de la révolution numérique dans la conduite des opérations militaires (drones, robots, intelligence artificielle, connectivité...).

Dans le registre des *télécommunications*, le projet américain de Greg Wyler (ancien ingénieur de Google, à la tête de la société OneWeb) de lancer à horizon 2019 plusieurs centaines de satellites (900 satellites pesant moins de 150 kilos contre 5 tonnes pour les satellites de télécoms actuels) en orbite basse pour fournir un accès à Internet préfigure également une autre révolution à venir en matière d'accès à Internet et d'augmentation des débits. D'autres projets d'Internet par l'espace pourraient également voir le jour, notamment avec Elon MUSK (créateur de Paypal, actuel P-DG de Tesla et de Space X qui

envoi déjà des fusées dans l'espace pour la NASA) qui envisage, avec le soutien financier de Google, d'envoyer 4000 petits satellites et de les interconnecter avec des rayons laser.

Le *Big et Fast Data* et l'*internet des objets (IdO)*. L'explosion quantitative de la donnée numérique contraint à de nouveaux ordres de grandeur qui concernent la capture, le stockage, la recherche, le partage, l'analyse et la visualisation des données. Les prochaines guerres seront très certainement en partie remportées par ceux qui seront en mesure de mieux contrôler, analyser, exploiter, protéger et attaquer une somme de plus en plus importante d'information. A l'instar du *cloud* civil, l'ensemble des vecteurs, effecteurs et structures de commandement connectés fera appel au *cloud* militaire (ou *combat cloud*) qui réduira la ségrégation naturelle entre chaque milieu (terrestre, maritime, aérien et espace) et qui permettra de compresser et d'accélérer la boucle décisionnelle (boucle Observation, orientation, décision, action – OODA) et le cycle de ciblage.

Le *Big et Fast Data* et la géo-distribution (répartition des ressources disponibles entre des *datacenter*^[6]) centralisés, décentralisés et jusque dans les terminaux mêmes des utilisateurs) vont considérablement faire évoluer le *cloud computing*^[7] et donc le *combat cloud* à horizon 2030. Selon certaines estimations, 40 zétaoctets de données (40000 milliards de gigaoctets) seront créés à horizon 2020, en grande partie générés par les 30 milliards d'objets connectés (informations provenant des messages envoyés, vidéos publiées, informations climatiques, signaux GPS, enregistrements transactionnels d'achats en ligne...). Le volume de données qui sera généré dans le secteur de la défense (ne serait-ce qu'au travers de la fonction *Intelligence, surveillance et reconnaissance – ISR*) sera tout aussi exponentiel dans les années à venir. L'essor des applications tirant partie en flux tendu de ces données exigera des traitements extrêmement rapides et donc au plus près des utilisateurs.

Ces évolutions numériques majeures ouvrent donc la voie à un *environnement pervasif et ubiquitaire* et un monde dans lequel les objets et les individus pourront communiquer et se localiser à tout moment avec les autres éléments, quel que soit leur « milieu de rattachement » (terrestre, aérien, maritime et espace). Les enjeux liés au *combat cloud*, c'est-à-dire à la maîtrise et à la gestion des données (transport, stockage, management, analyse, sécurisation, disponibilité...) sont ainsi au cœur des défis à relever.

Le cyberspace, nouvel espace de confrontation

Le Cyberspace, un milieu à part entière, fédérateur des autres milieux

Le *cyberspace* est une métaphore souvent utilisée pour rendre plus facilement compréhensible l'expansion rapide des technologies numériques et la place qu'elles occupent désormais dans nos vies.

Le *cyberespace* (défini par l'Agence nationale pour la sécurité des systèmes d'information – ANSSI comme « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ») est donc tout naturellement un espace de compétition et de confrontation pour l'ensemble des activités qui sont nées et vont naître de la révolution numérique. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme, criminalité et sabotage trouvent dans le cyberespace un nouveau champ d'expression.

Le cyberespace s'articule autour de trois couches : *la couche physique* qui comprend les éléments matériels et les éléments actifs (câbles sous-marins, fibres optiques, satellites, serveurs, routeurs, ordinateurs...), *la couche logicielle ou applicative* (systèmes d'exploitations, logiciels, protocoles...), qui concentre près de 80% des attaques informatiques, et *la couche sémantique* de l'information et des perceptions qui s'attache au sens contenu dans l'information.

Le cyberespace, comme l'environnement électromagnétique, supporte une quantité grandissante d'applications numériques civiles et militaires indispensables à de vastes pans d'activités économiques et régaliennes. Dans la sphère militaire, de nombreuses capacités opérationnelles reposent désormais en très grande partie sur l'usage et la maîtrise du cyberespace (et de l'environnement électromagnétique). Or, ce nouveau champ de confrontation se distingue par son *caractère transverse aux autres milieux*. Le *cyberespace donne corps à un environnement pervasif et ubiquitaire*. *De facto*, toute opération dans le champ du numérique doit donc viser à faciliter les opérations dans les autres environnements opérationnels (terrestre, maritime, aérien et espace).

Dans ce nouvel espace de confrontation, la supériorité opérationnelle ne pourra être obtenue qu'à condition de s'approprier les *game-changers* technologiques de la révolution numérique (robotique, IA, cyber, fabrication additive, IdO, *Big et Fast Data*...) et de faciliter la coopération de l'ensemble des acteurs prenant part au combat et au règlement d'une crise.

Ces *game-changers* technologiques offriront à terme des capacités de compréhension et de modélisation de l'environnement des opérations militaires. Ils donneront la possibilité pour le chef militaire de faire face à la surprise, de réagir devant l'imprévu, d'influencer son adversaire en agissant sur les perceptions (au travers de véritables batailles narratives dans un champ informationnel qui va gagner en intensité), et donc de provoquer la surprise en se rendant imprévisible, grâce à ses propres capacités d'adaptation. Les actions coordonnées dans le cyberespace *démultiplieront l'efficacité des actions classiques dans les autres milieux*.

Plus encore, la quantité d'information qui sera générée sur le champ de bataille, la puissance de calcul, les capacités de traitement informatique et les algorithmes prédictifs vont devenir le nerf de la guerre et les outils de modélisation-simulation-optimisation (MSO) ainsi que les

modèles d'aide à la décision et à la compréhension ouvriront la voie à une nouvelle forme de *guerre prédictive*^[8]. Dès lors, les synergies et la coordination étroite entre les acteurs du renseignement en amont, les différents échelons de commandement et les effecteurs dans chaque milieu seront au cœur des enjeux militaires à venir pour faire du *cyberespace un véritable espace fédérateur des autres champs traditionnels de confrontation*.

Le Cyberespace, une menace réelle, permanente et croissante

Quelques exemples récents illustrent les menaces réelles qui pèsent sur l'ensemble de nos secteurs d'activités : en décembre 2016, des hackers s'en prenaient ainsi au réseau de distribution électrique ukrainien, plongeant la moitié des foyers de la région d'Ivano-Frankivsk (1,4 million d'habitants au total) dans l'obscurité. L'année précédente, les autorités allemandes révélaient que de mystérieux pirates informatiques étaient parvenus à prendre le contrôle à distance d'un haut-fourneau, le poussant à une telle température que l'équipement industriel avait été irrémédiablement endommagé. Le piratage, au printemps 2016 d'une centrale nucléaire allemande a fait grimper d'un cran les craintes des experts occidentaux en cyber sécurité face à des commandos numériques difficiles à identifier avec exactitude. Très souvent les regards se tournent cependant vers Moscou, tout comme lors de la campagne présidentielle américaine où des hackers russes s'en seraient pris aux serveurs du comité national démocrate, chargé de lever des fonds en faveur d'Hillary Clinton et sont ainsi soupçonnés d'avoir pu influencer les résultats des élections de la plus grande démocratie occidentale.

Ces incidents vont donc au-delà des simples actes de sabotage et visent à affirmer une forme de puissance et un pouvoir de nuisance susceptibles de peser dans des relations diplomatiques de plus en plus conflictuelles^[9]

Avec une hypothèse de 20 à 30 milliards d'objets connectés à horizon 2020 et l'apparition de nombreux acteurs (États, GAFAM, groupes terroristes, organisations intermédiaires de type *proxy* (Le terme de Proxy est à prendre au sens du rôle d'intermédiaire, en se plaçant entre deux hôtes pour faciliter ou surveiller des échanges.)), cybercriminels, hackers, mouvement cyber militant de type Anonymous...), la menace cyber est donc plus que jamais devenue une réalité qui ne peut que s'intensifier, se diversifier et face à laquelle les armées et la France se sont déjà mises en ordre de marche.

Une réponse et une organisation complète qui devra évoluer face aux enjeux à venir

Déjà identifiés dans le Livre blanc de 2008, les menaces et les risques induits par l'expansion généralisée du cyberespace ont été confirmés dans celui de 2013. Une véritable dynamique existe au sein du ministère de la défense (MINDEF) autour des activités du numérique et du cyber espace. Un nombre important d'acteurs, d'organismes et de ressources ont été créés et mis en place pour couvrir l'ensemble du périmètre lié au numérique et au cyberespace. Pour autant, le paysage semble parfois *disséminé, voire compartimenté et segmenté*.

Une organisation complète mais disséminée et compartimentée

Un Officier général transformation digitale des Armées (OGTDA) a été créé à l'automne 2016 à l'Etat-major des armées pour en accélérer la transformation digitale, préserver la supériorité face à un ennemi évoluant dans l'espace numérique et rechercher l'efficacité dans le domaine organique et fonctionnel, dans un contexte de ressources (financières et humaines) contraint.

Une *direction bicéphale des systèmes d'information (DSI)*: à côté d'une *Direction générale des systèmes d'information et de communication (DGSIC)* ministérielle, davantage tournée vers la normalisation et la coordination interministérielle, la *Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI)* est en lien étroit et constant avec l'ensemble des armées directions et services (ADS) qui réclament des systèmes d'information configurables, à la fois pour leurs activités fonctionnelles/métier (Systèmes d'information d'administration et de gestion-SIAG) mais aussi pour l'emploi opérationnel des forces (Systèmes d'information opérationnel et de commandement-SIOC).

Pour chaque ADS, l'enjeu des NTIC est véritablement la création de valeur et de nouveaux usages pour les différentes chaînes fonctionnelles (métiers). La notion de sécurité est primordiale, d'autant plus que les données sont convoitées et que les nouvelles façons de travailler (cloud, mobilité et nouveaux supports de type smartphones/tablettes) accentuent les risques. Véritable opérateur des systèmes d'information du MINDEF, la DIRISI accompagne les ADS sur l'utilisation des nouvelles technologies, sur la gestion des risques et la notion de conformité légale de l'usage qu'ils en font. Dans la numérisation et la transformation du MINDEF par les systèmes d'information et de communication (SIC), le rôle du DIRISI prend une nouvelle dimension, en complémentarité de l'OGTDA.

La *Direction générale pour l'armement Maîtrise de l'information (DGA-MI)* apporte au MINDEF l'expertise technique dans les domaines des systèmes d'information et de communication, de la guerre électronique, les systèmes de missiles tactiques et stratégiques et du cyber.

Enfin pour compléter ce paysage ministériel, un *officier général Cyber* est en place depuis 2011, précurseur du *commandement de cyberdéfense et des opérations cyber*. Le 12 décembre dernier, M. Jean-Yves Le DRIAN posait en effet les bases d'une doctrine renouvelée de la cyberdéfense et annonçait la création à l'été 2017 d'un *commandement de la cyberdéfense*. Récusant toute idée de dissuasion conventionnelle ou cyber, M. Le DRIAN a rattaché les problématiques cyber aux questions d'ordre conventionnel et a posé les bases de ce que pourrait être une doctrine et une stratégie cyber de la défense afin de mieux intégrer l'ensemble des volets cyber dans la pensée militaire.

Ainsi, trois missions principales sont assignées au domaine cyber. En premier lieu le *renseignement* qui a pour objectif de contribuer à identifier nos failles et vulnérabilités, de

détecter et caractériser les actions hostiles, d'en attribuer l'origine, de participer aux actions de remédiation et de contribuer à préparer les réponses offensives. En second lieu *la Posture de Protection/Défense*, qui comprend la *posture permanente cyber* (mesures réduisant les risques sur nos systèmes dont ceux des opérateurs d'infrastructures vitales), la *défense en profondeur* (ou cyber protection) et la *défense de l'avant* (ou lutte informatique défensive). Enfin, troisième mission, la *lutte informatique offensive* (entraver, neutraliser, riposter), qui doit permettre d'agir contre un ennemi cherchant à nuire à nos intérêts de sécurité et de défense.

La création d'un commandement de la cybergdéfense qui conforte les structures existantes et consolide les ressources allouées au sein du MINDEF est-elle pour autant à la hauteur des enjeux à venir pour mener les opérations militaires dans l'espace numérique à horizon 2030 ?

Vers l'émergence d'une véritable armée numérique

Il existe encore de multiples acteurs qui agissent directement ou indirectement sur au moins l'une des trois couches du cyberspace et concourent à la fonction/communauté *C5ISR* (Command, Control, Computer, Communications, *Cyber*, Intelligence, Surveillance, Reconnaissance). Il y a historiquement et logiquement une dissémination et un cloisonnement (organisation en strates et en tuyaux d'orgue) entre l'ensemble de ces principaux « acteurs numériques » qui constituent le noyau dur de la fonction *C5ISR*, selon leur armée d'appartenance, leur milieu (terrestre, maritime, aérien, espace) et niveau d'emploi (stratégique, opératif et tactique). Etats-majors opérationnels, management de l'information, *data management*, SIC, *Cyber*, guerre électronique (GE), gestion et exploitation du spectre électromagnétique, renseignement d'origine électromagnétique (ROEM), renseignement d'origine image (ROIM), renseignement d'origine cyber (ROC), stratégie militaire d'influence et opérations d'information... sont autant de fonctions et d'acteurs dont l'action mérite d'être mieux coordonnée et *intégrée* pour favoriser les synergies.

Il appartient dès lors de traiter les « formes d'antagonismes » qui peuvent exister entre tous ces acteurs en adaptant l'organisation et les compétences pour lutter efficacement contre les enjeux de pouvoir et de territorialité qui peuvent prévaloir, à la fois entre les ADS mais aussi entre les niveaux stratégiques, opératifs et tactiques.

Une armée numérique, pour quoi faire ?

Le modèle actuel d'organisation de nos armées ne doit pas être un frein pour relever les défis de la révolution numérique. Garante d'une meilleure *convergence et intégration* de l'ensemble des capacités, la mise en place d'une véritable armée numérique doit offrir la faculté d'agir et de combattre conjointement pour relever un double défi : celui de la

maîtrise d'une ressource humaine rare et convoitée et celui d'une meilleure efficacité opérationnelle.

Relever un enjeu RH majeur

Les transformations numériques actuelles et à venir suscitent de fortes attentes de profils hautement qualifiés et feront émerger de nouvelles compétences et de nouveaux métiers. *Chief data officer, data scientist, data protection officer, community manager, web project manager, digital brand manager, chief data officer...* Pour ne citer que l'exemple du *Big et Fast Data*, le *data scientist* est chargé de « faire parler » les données et de les présenter sous un format simple. Le *data protection officer* est, quant à lui, garant de la protection des données sensibles au sein de son organisation. Autant de nouveaux métiers qui apparaissent en plus des métiers techniques liées aux NTIC elles-mêmes.

Pourtant, selon une étude Eurostat, 42 % des entreprises françaises rencontrent des difficultés pour recruter des spécialistes du numérique. La formation dans ces domaines est encore balbutiante et insuffisante. Le besoin des entreprises en *data scientists* est évalué entre 5 000 et 10 000 recrutements par an, alors que l'offre serait d'à peine 300 diplômés. De plus, les employeurs recherchent souvent une double compétence NTIC et métier (statistiques, mathématiques mais aussi développement, marketing...) ce qui rend le recrutement d'autant plus compliqué.

La défense n'échappe bien évidemment pas à cet enjeu majeur. Il est indispensable de bien appréhender les transformations en termes de RH qui découlent de la révolution numérique et du cyberspace pour se doter et mettre en œuvre les outils adéquats : modes de recrutement et rémunérations adaptés et capables de répondre à la concurrence, parcours professionnels attractifs (reconversion incluse) et favorables à la fidélisation du personnel (mobilité, validation des acquis et de l'expérience), équilibre entre les différentes catégories de personnel (civil et militaire), adaptation des statuts...

Plusieurs initiatives au sein du ministère de la défense sont à relever dans ce domaine: le pôle d'excellence cyber, le réseau cyberdéfense de la réserve citoyenne, le projet d'*Intelligence campus* de la Direction du renseignement militaire (DRM) ou encore tout dernièrement la création d'un Brevet de technicien supérieur (BTS) cyber au Lycée militaire de Saint Cyr L'école. Autant d'initiatives qui préfigurent ce que pourrait être une véritable « École 42 » de la défense, à l'instar de l'école française d'informatique privée créée par Xavier NIEL (à l'origine de l'offre d'accès à Internet sous le nom de Free à la fin des années 90), qui applique les principes de l'économie collaborative à l'éducation et à la formation.

La création d'une armée numérique doit donc participer en tout premier lieu de cette volonté d'optimiser une ressource humaine tendue (parce que rare et sous dimensionnée), volatile (parce que soumise aux évolutions technologiques rapides et incessantes) et très convoitée par un secteur privé plus rémunérateur. Anticiper les besoins en compétences,

développer une gestion prévisionnelle des emplois, des effectifs et des compétences (GPEEC), recruter de nouveaux agents et fidéliser les meilleurs malgré la concurrence des entreprises privées, améliorer les rémunérations des agents non titulaires et des militaires sous contrat sont autant de défis RH à relever.

Garantir la supériorité opérationnelle

Comme le rappelle M. Le DRIAN, « face à une attaque (*ndlr* cyber), il conviendrait que nous puissions proposer au Président de la République un large éventail de réponses possibles, sans nous limiter par avance à la sphère militaire ni au domaine cyber ».

La création d'une armée numérique doit donc également concourir directement à un double objectif : se doter d'une véritable capacité et liberté de manœuvre dans le cyberspace et être à même de mieux planifier et coordonner les actions dans le champ du numérique en appui de la manœuvre globale dans les autres environnements opérationnels en *intégrant* davantage les acteurs de la fonction C5ISR.

La numérisation offrira à terme les bénéfices escomptés à nos structures de commandement qui gagneront en agilité, en performance et en efficacité en surmontant le risque de saturation informationnelle.

L'armée numérique de demain devra concourir à fluidifier le renseignement et le rendre plus accessible aux échelons opératifs et tactiques. Si les flux informationnels et numériques peuvent brouiller davantage la compréhension et l'appréciation de situation, l'automatisation du traitement des données et la croissance de la puissance de calcul permettront d'innover les forces et leurs effecteurs jusqu'au plus bas échelon pour répondre au besoin tactique d'immédiateté et de précision.

Pour conforter cette supériorité opérationnelle, cette construction *ab initio* d'un nouveau modèle d'armée numérique repose sur deux facteurs clés de succès : elle doit d'une part renforcer la performance des structures de commandement et d'autre part décloisonner et fluidifier les liens entre les acteurs du renseignement, les structures de commandement et les effecteurs.

Armée numérique vs armées numériques : quel format et quelle organisation ?

Il s'agit donc dès à présent de dessiner les contours d'un *modèle d'intégration* capable de tirer le meilleur parti des impacts à venir de la révolution numérique. S'appuyant à la fois sur l'axe d'intégration vertical (selon le niveau d'emploi : stratégique, opératif ou tactique) et horizontal (par milieu : terrestre, maritime, aérien et espace), l'armée numérique de 2030 devra donner corps à une *fonction C5ISR structurée et cohérente*.

C'est donc bien sur le *degré d'intégration* souhaité et réaliste que les trois scénarii qui suivent invitent à porter plus en avant la réflexion.

Scénario 1 : une armée numérique concentrée autour d'un acteur organique unique

A l'instar du modèle allemand mis sur pied au second semestre 2016 (création d'une composante et d'une direction générale *Cyber/Information domain*), la France pourrait prendre l'initiative de regrouper sous un commandement organique unique les principaux acteurs de la fonction C5ISR (SIC, cyber, ISR stratégique, ROEM et ROIM, stratégie militaire d'influence et opérations d'information, géographie selon le *benchmark* du modèle allemand).

Cette nouvelle structure aurait pour finalité première de décroiser l'organisation en tuyaux d'orgue actuelle en concentrant plusieurs leviers d'actions aux mains d'une véritable *autorité fonctionnelle unique du domaine C5ISR*: doctrine, organisation, gestion des ressources (humaines : recrutement, plan de carrière, formation, réserve opérationnelle et citoyenne...) et financières (pouvoir adjudicateur), gestion de biens, préparation à l'engagement opérationnel pour les niveaux stratégiques et opératifs...

Une telle structure offrirait l'avantage de donner une compétence RH à ce nouvel acteur pour lui permettre de mieux coordonner les ADS. A contrario, les lignes de partage de responsabilités devront être clairement définies entre ce nouvel acteur, les ADS et la chaîne de conduite des opérations pour éviter de créer une technostructure sans âme ni conscience qui sépare et éloigne les acteurs numériques des armées.

Scénario 2 : une armée numérique concentrée autour d'un contrôleur opérationnel (OPCONer) interarmées unique

A l'instar du Commandement des opérations spéciales (COS), la France pourrait regrouper sous un commandement opérationnel interarmées unique l'ensemble des composantes C5ISR qui resteraient organiquement rattachées à leurs armées d'origine.

Ce modèle d'organisation concentré autour d'un *OPCONer* interarmées unique doit permettre d'accroître la performance du commandement et d'optimiser la coordination des opérations. Cette centralisation doit favoriser l'intelligence et l'appréciation de situation ainsi que l'accélération des processus décisionnels. Une action interarmées coordonnée et centralisée offre une meilleure garantie de conquérir la supériorité cybernétique et électromagnétique.

Une telle organisation offrirait au chef militaire en charge des opérations sur un théâtre la possibilité de disposer d'une articulation des moyens lui conférant une très grande agilité pour *distribuer dans différents milieux* des opérations variées dans des créneaux contraints.

Scénario 3 : une armée numérique disséminée autour de plusieurs acteurs « intégrables à la demande ».

A contrario, le principe de subsidiarité entre les échelons stratégiques, opératifs et tactiques doit permettre d'éviter le piège d'une centralisation excessive et la saturation des échelons de commandement et de coordination.

Les *game-changers* de la révolution numérique doivent permettre d'envisager une déconcentration de l'organisation du commandement et de coordination des différents acteurs à l'échelon opératif et tactique. Un modèle déconcentré pourra offrir une plus grande réactivité à condition de mettre en place les structures de coordination *ad hoc*^[10] permettant d'accroître la synergie des actions et optimiser les effets obtenus. Un tel modèle pourrait ainsi conduire à de véritables *opérations distribuées*, décentralisées dans la profondeur, avec une forme de *commandement ubérisé de type C to C*^[11]

La contraction des délais décisionnels pour saisir les créneaux d'opportunité nécessite à la fois un bon niveau de délégation de l'échelon stratégique à l'échelon opérationnel, mais aussi un rapprochement d'exercice des responsabilités des niveaux opératifs et tactiques, et ponctuellement de privilégier une compression de ces deux niveaux hiérarchiques^[12]. Un modèle d'armées numériques déconcentrées au niveau des armées, selon une logique de milieux, devra donc reposer sur des structures de commandement opérationnel allégées et plus agiles, avec une empreinte au sol réduite et une mobilité accrue qui favoriseront l'appréciation de situation et la prise de décision en temps réel.

Chacun de ces trois scénarii reste bien évidemment modulable et peut faire l'objet de combinaisons et d'adaptations. Le premier modèle consistant à créer une autorité organique centralisée unique peut par exemple voir ce rôle dévolu à l'une des trois armées, dont les caractéristiques de milieu s'apparenteraient le plus à celles du cyberspace. Le troisième modèle décentralisé peut quant à lui se voir adjoindre la création d'une autorité fonctionnelle chargée de coordonner l'ensemble des acteurs déconcentrés pour faciliter leur intégration au cas par cas. Quant au second modèle, rien ne l'empêche d'évoluer dans le temps pour se rapprocher du modèle déconcentré au fur et à mesure que les ruptures technologiques faciliteront le principe de subsidiarité et la conduite d'opérations distribuées.

L'adaptation de notre outil de défense aux défis posés par la révolution numérique repose en partie sur l'analyse et la compréhension des courants ou signaux faibles qui sont annonciateur des grandes ruptures technologiques à venir. Il est important d'identifier dès à présent la fenêtre d'opportunité et de définir le rythme et la trajectoire de la transformation en profondeur qui amènera, le moment voulu, à la création d'une forme d'armée numérique dont le contour et le mode de fonctionnement restent à inventer.

Les germes de rupture résident souvent dans l'attentisme et une confiance excessive dans notre outil de défense. La préparation aux grandes ruptures à venir nécessite donc un effort permanent d'anticipation et d'imagination pour ne pas reproduire les schémas et les modes de pensée figés et surannés.

Pour relever efficacement les défis du numérique et affronter les menaces du cyberspace, il convient de cultiver notre résilience et notre capacité d'adaptation et de création au plan militaire. Quelle que soit la forme choisie et le niveau d'intégration retenu, la mise sur pied d'une véritable armée numérique repose ainsi sur la capacité à faire davantage converger dès à présent l'ensemble des acteurs qui constituent la fonction C5ISR.

Cette armée numérique tirera le meilleur parti des ruptures technologiques à venir et créera les conditions pour transformer le cyberspace en *cet environnement pervasif et ubiquitaire, fédérateur des autres champs traditionnels de confrontation*. Elle favorisera la continuité entre les éléments techniques, organiques et opérationnels. Elle permettra de mieux combiner l'innovation technologique, stratégique et tactique et fera écho à Antoine de Saint Exupéry qui disait : « pour ce qui est de l'avenir, il ne s'agit pas de le prévoir mais de le rendre possible ».

Document 3 : « Le numérique, au cœur des priorités du SCA » - portail-commissariat.intradef.gouv.fr

Le numérique, au cœur des priorités du SCA

Confronté à des problématiques récurrentes de recrutement de profils experts en conduite de projets SIC (systèmes information communication), le ministère des Armées, via le Centre de Formation de la Défense, propose une alternative novatrice en s'engageant dans une formation spécialisée au profit de ses propres ressortissants.



Cette initiative s'inscrit dans le cadre de chantiers ministériels (académie du numérique, politique de formation ministérielle) pleinement pris en compte par le Service du commissariat des armées (SCA) dans ses schémas directeurs numérique et de formation employeur.

Ce dispositif de formation de courte durée (40 demi-journées), accessible sur volontariat, est proposé en e-learning.

Il vise en cible :

- en opportunité : à redéployer des agents sur de nouvelles missions dans une logique de reconversion

ou

- en gestion de projet : à optimiser des compétences internes.

Les employeurs du MINARM disposent dorénavant d'un levier intéressant pour conserver une capacité à manager des projets SI (systèmes d'information) qui nécessitent un pilotage opérationnel efficace. De leur côté, les agents pourront ainsi valoriser leur parcours dans l'institution avec en particulier l'opportunité d'obtenir des certifications techniques reconnues en fin cycle.

La session de formation 2021 composée de 10 personnels civils et militaires est proposée dans un cadre expérimental ouvert exclusivement aux agents disposant d'un profil SIC.

Le SCA s'est d'ores-et-déjà positionné dans le cadre de cette première session de formation qui débutera à la fin du mois de septembre 2021 avec la participation de deux agents de deux centres interarmées du soutien (CIRL et CISAP) impliqués dans des projets SI relatifs aux domaines « RHL » et « Solde ».

L'ambition à partir de 2022 sera de panacher les profils SIC/non-SIC avec deux nouvelles sessions proposées puis trois par à compter de 2023.

Il est rappelé que les besoins en formation SIC s'expriment essentiellement au titre du plan annuel d'enrichissement des ressources humaines par la formation (PERF) – plan de formation métier du SCA :

- s'agissant des personnels civils : concomitamment aux entretiens effectués dans le cadre des CREP annuels (période de janvier à mars) ;
- s'agissant des personnels militaires : dans le cadre de la diffusion du catalogue de formations par les responsables de formation (traditionnellement en début d'année).

Des besoins avérés peuvent également être pris en compte au fil de l'eau, indépendamment de ce plan.

En attendant, bien que l'intégration de cette formation dans le catalogue SCA ne soit pas encore effective à date [elle le sera en 2022], les organismes intéressés pour engager l'un de leur(s) agent(s) dans ce dispositif en 2022 sont invités à se rapprocher de leur responsable de formation qui prendra attache avec le pôle numérique au besoin.

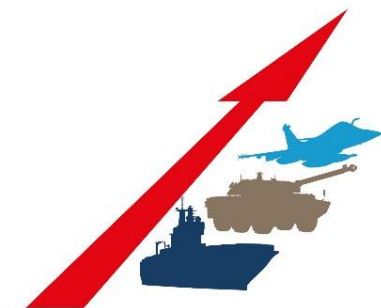
Document 4 : « Qu'est-ce que la transformation numérique ? » - portail-transformation-numerique.intradef.gouv.fr

La société vit aujourd'hui une transformation d'ampleur, celle du **numérique**. Initiée au début des années 2000 avec la **démocratisation d'Internet** et la commercialisation des premiers **smartphones**, la transformation numérique a, en l'espace de **deux décennies**, profondément modifiée nos modes de vie en permettant l'émergence de **nouveaux usages**.

La **transformation numérique** se couple à une accélération sans précédent de nos **modes de vie**. L'expérience de l'immédiateté rend les **utilisateurs** plus **exigeants** et plus **impatients**, le rythme des ruptures technologiques s'accélère et les usages sont sans cesse renouvelés.

La transformation numérique est un moteur de transformation puissant pour le monde du travail, pour l'administration et plus largement pour les mécanismes de prise de décision. Sous l'impulsion de Florence Parly, le ministère des Armées s'inscrit dans une **démarche volontaire** qui vise à générer des ruptures dans les usages et les modes de travail, en s'appropriant au plus vite et dans les meilleures conditions les technologies émergentes et **innovations numériques**, avec pour objectif **de mieux remplir ses missions**.

L'Ambition numérique définit 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

1.5.

1.6. « Une ambition qui vise à bâtir un ministère des Armées pleinement entré dans le XXI^e siècle, pleinement attractif et pleinement opérationnel. Une Ambition qui vise à bâtir un ministère numérique. » Florence Parly, ministre des Armées



Portée par les métiers dont il faut outiller le foisonnement d'idées, basée sur des principes de **subsidiarité, de co-construction et d'ouverture vers l'extérieur**, la transformation numérique du ministère donne notamment une place centrale à l'utilisateur, à l'utilisateur : simplification et numérisation des démarches administratives, accompagnement des agents et de leurs familles.

L'*Ambition Numérique* a été concrétisée en avril 2018 au travers du **Schéma directeur de la transformation numérique – Défense Connect**, qui permet d'orienter les initiatives à travers huit objectifs métiers évolutifs, ainsi que d'aider les métiers dans leur transformation en leur apportant les outils indispensables pour relever les défis de la compétence, de la rénovation du socle du système d'information ministérielle et celui de la donnée. Trois défis structurants de la transformation numérique du ministère.

Enfin, la **création d'une Direction générale du numérique et des systèmes d'information et de communication (DGNUM)** en juin 2018, directement rattachée à la ministre, apporte au processus une fonction de chef d'orchestre en capacité de porter les sujets transverses, d'orienter et de soutenir les projets des métiers, tout en assurant la cohérence globale des systèmes d'information et de communication. La **donnée étant au cœur de la transformation numérique**, le DGNUM assume ainsi la fonction d'administrateur ministériel des données avec pour mission de coordonner les actions de gouvernance du ministère dans le domaine de la production, de la circulation, de l'exploitation, de la protection, du partage et de la diffusion des données.

Document 5 : « Optimiser l'exploitation des données dans le secteur public » - www.bearingpoint.com

Alors que la consultation publique sur l'avant-projet de loi pour une République numérique s'est achevée le 18 octobre, les administrations doivent prendre conscience des opportunités offertes par la publication et la massification des données, ainsi qu'adopter une stratégie ambitieuse en la matière. Comme l'a récemment rappelé l'OCDE, l'Open Data et les Big Data constituent des ressources uniques dont le secteur public peut tirer profit dans l'exercice de ses missions. Une utilisation élargie et réfléchie des données peut notamment aider les administrations à :

- **Améliorer la qualité du service public rendu aux usagers.** Une architecture de données performante est à même de faciliter les démarches des citoyens dans leurs relations avec l'administration. Le partage de données inter-administrations peut par exemple permettre aux usagers de disposer de formulaires pré-remplis avec leurs données, afin d'éviter des actions répétées et chronophages.
- **Renforcer la transparence du secteur public.** La simplification et la modernisation de l'accès aux données publiques passent par un recours accru aux outils numériques. Il s'agit d'améliorer l'accessibilité et l'intelligibilité de certaines données détenues ou générées par les administrations. Cette mise à disposition de données peut en retour favoriser la compréhension et l'acceptation des politiques publiques par les citoyens.
- **Elaborer les politiques publiques :** les Big Data ouvrent de nouvelles perspectives pour décrire la réalité et formuler des prévisions. Elles peuvent donc permettre des prises de décision étayées par des informations plus précises et plus fiables. L'utilisation de données peut ainsi trouver des applications dans de nombreux domaines, tels que la santé publique, la politique de l'emploi, l'environnement ou encore la lutte contre la criminalité et les fraudes.
- **Evaluer l'impact des politiques publiques** et calibrer les réponses adéquates, via l'analyse de données en temps réel et leur mise en relation avec les objectifs initiaux des décisions.

Les données offrent ainsi de nombreuses possibilités d'applications au secteur public. A cet égard, la France a déjà pris des initiatives notables :

- La création d'un portail interministériel unique de partage des données publiques, administré par la mission Etalab au sein du SGMAP.
- La nomination d'un administrateur général des données, ce qui constitue une première pour un Etat européen. Ses missions couvrent notamment la définition d'une gouvernance des données, le contrôle de leur qualité et le développement de leur utilisation pour les politiques publiques.

- La participation à l'Open Government Partnership et la transmission dans ce cadre d'un plan d'action national en juillet 2015, qui comprend des engagements pour renforcer la politique d'ouverture et de circulation des données, et doit faire l'objet d'une première auto-évaluation en juillet 2016.

Grâce à ces évolutions, l'OCDE classe aujourd'hui la France au 2ème rang des Etats ayant le plus progressé en matière d'Open Data, juste derrière la Corée du Sud. Poursuivre et concrétiser ces efforts suppose notamment :

- **Des ressources humaines et technologiques** : la mise à profit des Big Data nécessite des outils élaborés permettant de stocker, analyser et représenter les données, ou encore de formuler des prévisions à l'aide d'algorithmes.
- **Un partage de données entre administrations** et le développement d'une culture collaborative : dans une logique de performance et de productivité, les données doivent pouvoir circuler au sein de la sphère publique, afin d'être consultées et réutilisées.
- **Une démarche de collaboration avec le secteur privé**, notamment pour bénéficier de ses capacités de collecte de données
- **Une gestion des risques** maîtrisée et une régulation proportionnée, afin de garantir la protection des données personnelles et confidentielles

Document 6 : « Secteur public : comment automatiser les processus mais pas leurs complexités ? » - www.hubinstitute.com

Secteur public : comment automatiser les processus mais pas leurs complexités ?

Par : Thibault Deschamps

2 mars 2020

Alors que la gestion publique est souvent pointée du doigt pour sa lourdeur administrative, le secteur public peut gagner en qualité et en performance grâce au Robotic Process Automation (RPA) ou automatisation des processus. Comment s'y prendre ? Éléments de réponse avec Dorothée Belle, Directrice Associée - Transformation du secteur Public, chez EY Consulting.

HUB Institute : Comment évaluez-vous la maturité du secteur public en matière d'automatisation des processus, comparé au secteur privé ?



Dorothée Belle, Directrice Associée - Transformation du secteur Public, chez EY Consulting : Il est certain que le secteur privé a un coup d'avance sur l'utilisation de ces innovations par rapport au secteur public. **Les secteurs bancaires ou du retail** notamment s'interrogent sur le potentiel de l'automatisation depuis des années et ont déjà dépassé le stade de l'expérimentation pour industrialiser.

Toutefois, les choses sont en train de changer à grande vitesse dans le secteur public. De nombreuses organisations (administrations centrales, collectivités locales, organismes de protection sociale...) passent aujourd'hui en revue leurs processus à l'aune de ces nouvelles technologies, pour exploiter les leviers digitaux et transformer la manière de délivrer leurs services aux usagers.

HUB Institute : Peut-on en déduire qu'on est encore loin de parler d'intelligence artificielle au sein des services publics ?

DB : Pour le moment, lorsque l'on parle d'automatisation des processus, **on parle surtout de robotisation (RPA)**. Ce sont deux choses très différentes. Le robot fait exactement ce qu'on lui dit de faire là où l'intelligence artificielle promet un algorithme permettant d'apprendre et in fine prendre des décisions.

Le RPA s'inscrit comme le premier levier d'une transformation data-driven des processus de décision de toute organisation, y compris publiques. Il permet de **considérablement réduire le temps que passent les forces vives aux tâches manuelles ou répétitives** afin de les consacrer davantage aux tâches à forte valeur ajoutée.










HUB Institute : Pourriez-vous nous citer deux cas d'usage concrets qui seraient considérablement optimisés par l'usage du RPA ?

DB : Si je prends comme exemple les collectivités locales et les départements, je pense immédiatement à tout ce qui concerne **les métiers du social**.

Ces derniers sont aujourd'hui confrontés à un paradoxe difficile à accepter pour les agents : alors même que leur cœur de métier doit être tourné vers la proximité et la relation à l'utilisateur, **le temps consacré à la saisie et à la vérification dans les outils informatiques devient de plus en plus important**. La faute à des volumes de données qui sont souvent extrêmement élevés.

Le développement des assistants digitaux apporte aujourd'hui une réponse innovante, souple et peu onéreuse pour réaliser de nombreux processus :

- **Saisie des informations reçues** depuis un formulaire en ligne dans un logiciel ;
- **Envoi de notifications** automatiques en masse ;
- **Contrôle automatique d'information** entre plusieurs outils, bases de données ;
- **Réalisation de calculs** dans un fichier Excel pour alimenter un système ;
- **Enregistrement de documents** dans une gestion électronique documentaire...

Quels processus automatiser ?								
								
Volumes élevés de saisies de données	Source d'erreurs humaines	Existence de règles de décision structurées	Nombreux processus manuels	Potentiel de gains financiers / manques à gagner importants	Contenu en données sensibles	Tâches à faible valeur ajoutée	Récurrence des activités	Tâches à réaliser pouvant être effectuées en dehors des heures ouvrées

On peut aussi évoquer tout ce qui concerne **les métiers de la finance et de la comptabilité**, avec des exigences toujours plus pressantes de payer vite et bien les factures reçues, tout en réduisant les risques d'erreur. L'automatisation est dans ce cas une réponse évidente pour gagner en performance opérationnelle.

HUB Institute : L'un des services publics les plus en difficulté reste l'hôpital. Comment le RPA pourrait l'aider ?

DB : Les hôpitaux sont effectivement parmi les organismes publics qui ont le plus à gagner en automatisant leurs processus. Vous avez aujourd'hui **un grand nombre de tâches administratives traitées par du personnel soignant**. En déléguant cette charge administrative, les hôpitaux peuvent redéployer ce temps gagné pour améliorer la prise en charge des patients.

Encore une fois, l'objectif final est de gagner en temps et en marge de manœuvres. Un enjeu crucial pour un service public souvent confronté au déficit de moyens humains et financiers.

HUB Institute : Automatiser des processus, n'est-ce pas risquer d'automatiser les problèmes ?

DB : Je suis bien d'accord. Comme nous l'évoquions précédemment, le robot se contente de dérouler **un processus normé et répondant à des règles de gestion précise**. Il ne faut donc pas automatiser la complexité !

Chez EY, nous avons la conviction que quel que soit le projet d'automatisation, l'application d'une nouvelle solution **doit être précédée d'une phase d'analyse critique, voire d'optimisation des processus**. Il faut toutefois noter que nombre de ces complexités sont dues au facteur humain, et plus précisément au fait que l'on affecte des ressources humaines à des tâches peu stimulantes.

On souligne ici une autre valeur du RPA qui permet de revaloriser des fonctions au sein des organisations.

HUB Institute : Et qu'en est-il de la relation humaine ? Intégrer robots et algorithmes, n'est-ce pas un pas vers la déshumanisation des relations entre l'administration et le citoyen ?

DB : Je ne le vois pas comme cela. **Les fonctions que l'on attribue aux automates ne sont pas relationnelles**. On tâche justement de réduire le temps dépensé par des ressources humaines à certaines tâches redondantes pour qu'elles puissent se concentrer sur l'amélioration du rapport humain et des prises de décision.

Reste toutefois à **apprendre aux agents à travailler aux côtés de ces nouvelles technologies**. Cette relation homme/machine doit être pensée au préalable pour tout projet et l'on ne décorrèle jamais la mise en place de ces innovations et

l'accompagnement des équipes. Les aspects RH et l'accompagnement au changement sont naturellement fondamentaux dans ces projets.

HUB Institute : Quelles sont les étapes capitales du déploiement d'une solution d'automatisation selon EY ?

DB : Les principales étapes pour déployer une solution de RPA sont les suivantes :

1 - Cadrage stratégique

C'est pendant cette phase que sont définis les objectifs à atteindre et les cas d'usage qui feront l'objet d'un développement prioritaire. L'objectif n'est pas tant de s'attaquer à toutes les complexités du processus, mais plutôt **d'identifier les plus lourdes**. C'est en réduisant ces dernières que **les bénéfices seront les plus importants à court terme**. De là il sera plus aisé d'étendre le projet à de nouveaux cas d'usages moins prioritaires.

En matière d'automatisation, EY a notamment l'habitude de mettre en place des Botathon. Ils prennent la forme de guichets nous permettant d'échanger avec l'ensemble des services et des acteurs de la chaîne de valeur en transformation.

L'enjeu est ainsi d'identifier le maximum de cas d'usages potentiels et d'aider nos partenaires à les prioriser. Bien sûr, ces informations viennent s'ajouter à notre expérience métier déjà très importante. Nous disposons d'une bibliothèque de connaissance déjà prête pour optimiser les processus des organisations publiques.

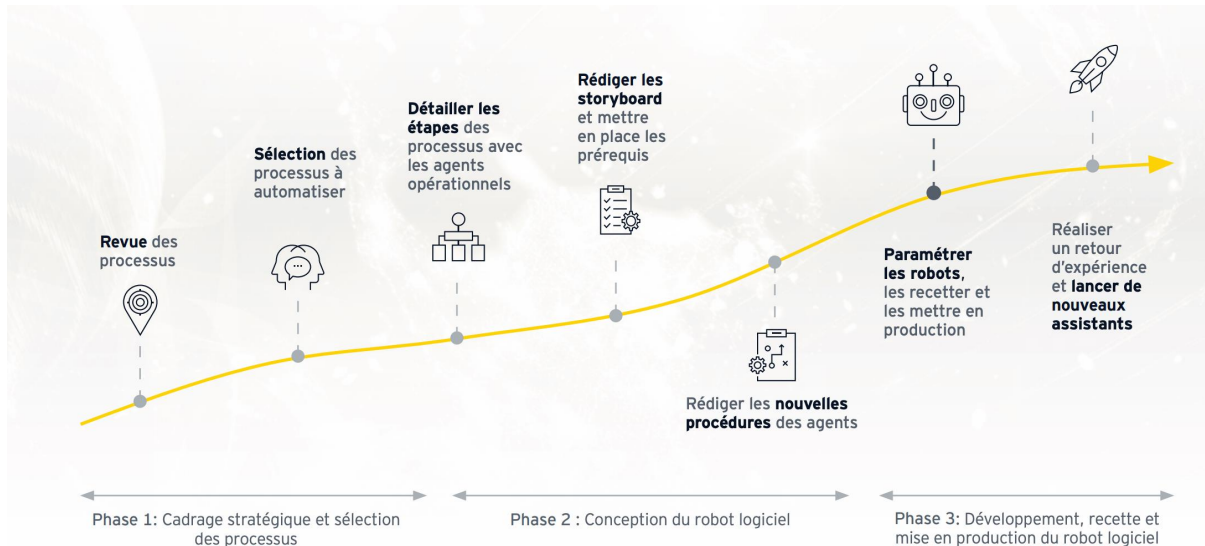
2 - Conception et développement

On entre ensuite dans la phase de conception du projet, et de conception du robot selon le cas d'usage pour lequel il sera déployé. Nous rédigeons concrètement ce que l'on appelle **des "user stories" décrivant, de manière très fonctionnelle et au clic près, tout le processus que devra réaliser le robot** à la place de l'humain. C'est sur la base de ce document validé que nous réalisons le développement des automates.

3 - Passage à l'échelle

Une fois que nous avons conçu la solution et l'avons testé en environnement contrôlé, nous collectons les premiers retours d'expérience. **L'objet est de modifier la solution si besoin est, ou, si tout est fonctionnel, de passer au déploiement**. Nous accompagnons ici nos partenaires dans la pose des robots (à la fois matériels et logiciels) dans leur écosystème, mais aussi dans le transfert des compétences qui permettront à ses équipes d'opérer la solution en totale autonomie.

Erreur !



HUB Institute : Quel est votre modèle économique, et à combien chiffrez-vous aujourd'hui les solutions de RPA ?

DB : La force d'EY c'est d'intégrer à la fois les compétences de conseil en automatisation et de déploiement à grande échelle de cette technologie. **Nous accompagnons nos clients de A à Z**, y compris sur le paramétrage, l'intégration et la maintenance des robots que nous déployons.

Il ne faut pas nécessairement un gros budget pour démarrer son projet, et une première vague complète peut être déployer en quelques mois dans **une enveloppe ne dépassant pas les 100 000 euros**.

Au-delà de la mise en place des automates, nous accompagnons nos clients publics sur l'ensemble de la proposition de valeur qui accompagne le projet : formation des acteurs et transfert de compétences, mise en place des centres d'excellence RPA chez nos clients, mise en place des outils et méthodes pour pérenniser et inscrire dans la durée cette nouvelle technologie dans l'architecture SI.

Document 7 : « SIRH 2022 : une feuille de route en 6 axes pour la transformation numérique de la fonction RH » - www.fonction-publique.gouv.fr

SIRH 2022 : une feuille de route en 6 axes pour la transformation numérique de la fonction RH



SIRH 2022. Derrière ce qui pourrait être un nom de code, en réalité une feuille de route ambitieuse déclinée en 6 axes stratégiques pour accompagner la transformation numérique de la fonction RH et ainsi contribuer à rénover le cadre des ressources humaines.

La transformation numérique de la fonction RH a fait l'objet de travaux interministériels menés dans le cadre de deux des cinq chantiers transverses du programme de transformation « Action publique 2022 » : « rénovation du cadre des ressources humaines » et « transformation numérique ». Ces travaux se sont appuyés sur les résultats du bilan d'étape du programme interministériel de modernisation SIRH-payé réalisé au deuxième trimestre 2017 et sur les perspectives proposées par les acteurs des systèmes d'information RH.

Le fruit d'une vision partagée

La Direction générale de l'administration et de la fonction publique (DGAFP) et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), avec l'appui de tous les acteurs concernés par les SIRH-Payé, ont élaboré, grâce à cette vision partagée des enjeux métier RH et des lignes directrices de la transformation numérique de l'État, une stratégie de transformation numérique de la fonction ressources humaines. Celle-ci doit permettre de consolider et optimiser les socles SIRH qui assurent la gestion administrative, la paye et le déclaratif, d'accompagner la poursuite de la professionnalisation des métiers et de la filière RH, de

développer de nouveaux services numériques RH en appui de la transformation du métier, d'améliorer le service rendu à l'agent, d'outiller le pilotage des ressources humaines.

6 axes stratégiques et des actions concrètes

Dématérialiser complètement les documents, fluidifier les processus, offrir de nouveaux services et usages, rendre les agents acteurs de leur gestion, disposer d'outils de pilotage performants et partagés... La feuille de route 2018-2022 comprend 6 axes stratégiques déclinés ensuite de manière opérationnelle.

- **Axe 1 - Poursuivre la consolidation des SIRH sur les fonctions socle de la gestion RH selon une trajectoire basée sur la convergence et la mutualisation des systèmes**

Les objectifs initiaux du programme SIRH-Paye (sécuriser la paye des agents de l'Etat, optimiser le processus de gestion administrative et de paye, améliorer les outils de pilotage de la masse salariale et des effectifs de l'Etat, moderniser la chaîne RH-Paye) gardent toute leur pertinence et leur nécessité. Mais les progrès réalisés doivent être amplifiés en accentuant la convergence progressive des SIRH-Paye et en améliorant la qualité des données RH. Il s'agit globalement d'optimiser l'efficacité des socles SIRH.

- **Axe 2 - Dématérialiser complètement les processus et les documents**

La dématérialisation constitue un levier essentiel de modernisation. Elle permet en effet de faciliter le partage et l'échange d'informations et de documents, d'envisager de nouveaux usages, et offre l'opportunité de revoir les processus et les organisations dans une optique de rationalisation, de simplification, d'enrichissement et d'ouverture des données publiques.

- **Axe 3 – Fluidifier les processus dans la logique du « Dites-le nous une fois »**

Les processus RH seront le plus possible simplifiés, dématérialisés, fluides, automatisés et intégreront le principe du « dites-le nous une fois ». Ils s'appuieront sur une numérisation aboutie des données et des documents.

- **Axe 4 - Offrir de nouveaux services et usages aux agents et aux acteurs RH - Rendre l'agent acteur de sa propre gestion**

Tous les utilisateurs des SIRH (agents gérés et acteurs RH) devront disposer de services RH numérisés de qualité se rapprochant de celle des services utilisés dans la sphère privée. L'agent deviendra acteur de sa propre gestion.

- **Axe 5 – Mieux maîtriser l'adéquation compétence requise / compétence détenue**

Des solutions numériques nouvelles et innovantes seront développées en appui au métier de la gestion des ressources humaines, en particulier dans le domaine de la GPEEC et de la gestion des talents, avec l'expérimentation d'outils et de suivi des compétences (via les entretiens d'évaluation ou des données déclaratives). Ces outils, reliés aux autres composants du SIRH permettront d'améliorer les parcours des agents et l'allocation des ressources humaines.

- **Axe 6 - Disposer d'outils de pilotage de la politique RH performants et partagés (SID)**

Les outils de pilotage ministériels et interministériels seront adaptés et développés selon une trajectoire cohérente et partagée entre les différents acteurs, mutualisant les indicateurs, les référentiels, les solutions et s'appuyant sur une plus large mobilisation des données existantes.