N° 996

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 30 mai 2018.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES

en conclusion des travaux d'une mission d'information [1]
sur les **enjeux** *de la* **numérisation** *des* **armées**

ET PRÉSENTÉ PAR

MM. OLIVIER BECHT ET THOMAS GASSILLOUD,
Députés.

[1] *La composition de cette mission figure au verso de la présente page.*

La mission d'information sur les enjeux de la numérisation des armées est composée de :

– MM. Olivier Becht et Thomas Gassilloud, *rapporteurs ;*

– MM. Luc Carvounas, Philippe Chalumeau, Alexis Corbière, Jean-François Eliaou, Jean-Jacques Ferrara, Jean-Christophe Lagarde et Fabien Lainé, *membres.*

SOMMAIRE

___

Pages

INTRODUCTION

Quelque nom qu'on lui donne, « révolution numérique », « mise en données » du monde (pour l'anglais *datafication*), « transition digitale » ou simplement « numérisation », le partage et le traitement de données en réseau s'imposent à tous – États comme individus, entreprises comme organisations publiques –, dans tous les champs de l'activité humaine – des tâches les plus banales du quotidien aux applications professionnelles les plus poussées. Plus qu'une technologie, c'est un phénomène qui sous-tend la marche de nos sociétés et les transforme en profondeur ; c'est tout un mode de vie qui change avec la technologie. En cela, peut-être, n'est-il pas abusif de parler de « révolution ».

Et encore, jamais révolution industrielle n'aura entraîné autant de bouleversements – et cela de façon aussi rapide – que l'essor du numérique, qui a profondément modifié en quelques années non seulement la production et la consommation de biens et services en tout genre, mais aussi jusqu'à nos manières d'interagir, d'apprendre et de penser.

Les armées ne sauraient, bien entendu, demeurer à l'écart de ces transformations. D'ailleurs, comment le feraient-elles ? C'est longtemps l'armement qui a donné l'impulsion dans l'innovation technologique et, si les armées ne sont plus les principaux prescripteurs de l'innovation technologique dans la « révolution numérique », en tout état de cause, elles font partie d'un écosystème humain, social, industriel et administratif traversé, comme l'ensemble de la société, par les mutations que suscitent les technologies numériques.

Cela vaut pour les armées comme pour toute organisation : la numérisation a profondément modifié les modes de production et de consommation, avec des gains de productivité dont les armées ne peuvent pas se priver dans le champ de leur activité dite « organique », c'est-à-dire celle du quotidien.

Cela vaut aussi dans le champ opérationnel, où nos armées occidentales se doivent de conserver la supériorité technologique qui fait leur ascendant opérationnel. Il s'agit dès lors pour elles, au travers des bouleversements technologiques à l'œuvre, de conserver et d'accroître toujours leurs capacités dans trois ordres de fonctions :

– identifier la menace, ce que les moyens numérisés doivent permettre de faire toujours plus rapidement, voire de façon prédictive ;

– neutraliser la menace, par un ensemble de moyens auxquels les technologies numériques peuvent conférer davantage d'efficacité, voire d'efficience, qu'il s'agisse d'armements classiques ou de combat cybernétique ;

– protéger les organes et systèmes d'importance vitale qui animent, irriguent ou innervent ce corps social complexe qu'est la Nation, à commencer par la sécurité de ses armes et de ses réseaux.

Le présent rapport dresse donc un état des lieux de l'appropriation des technologies numériques par les armées et, sur la base de ce constat, étudie comment celles-ci devraient consolider leurs acquis et relever les nouveaux défis que posent les ruptures technologiques envisageables dans le secteur numérique.

À l'étude, il apparaît que la France a plutôt bien engagé le « virage numérique » dans la mutation de ses armées, avec toutefois des succès qui restent inégaux. L'évolution rapide de nos alliés comme de nos potentiels adversaires, ainsi que les ruptures technologiques à venir, imposent aujourd'hui de faire de la numérisation de notre outil de défense une priorité nationale, sous peine de déclassement.

Il en ressort surtout qu'en fin de compte, les enjeux de la numérisation des armées s'analysent en réalité comme d'éminents enjeux de souveraineté. Souveraineté dans l'emploi de la force, bien sûr, mais souveraineté, aussi, dans la possession des technologies. Que l'on ne se leurre pas : bien loin des utopies qui ont pu présider, un temps, au développement de ces technologies, le numérique est bel et bien devenu un outil de puissance, un formidable levier au service de politiques de rayonnement et – on peut le dire sans hyperbole – de domination. L'industrie numérique est à ce titre un champ de rivalités entre des grandes puissances technologiques, parmi lesquelles les Européens ne figurent plus au premier rang.

C'est pour nos armées, instrument par excellence de notre autonomie stratégique, que la reconquête d'un plus haut niveau de souveraineté technologique est particulièrement cruciale. À l'heure du numérique, il n'y a pas de souveraineté possible en état de dépendance technologique.

C'est pourquoi les rapporteurs étudient les voies et moyens de la consolidation d'un écosystème d'innovation technologique à même de fournir la base industrielle et technologique de notre autonomie stratégique. Le ministère des Armées a un rôle majeur à jouer dans cet effort de consolidation. Et si, pour certains développements technologiques, l'échelle nationale paraît trop étroite, c'est dans l'optique d'une autonomie stratégique élargie à l'Union européenne que des efforts méritent d'être faits en coopération. Un tel effort suppose des investissements – tant financiers ou technologiques qu'humains – ainsi qu'une mutation de nos pratiques et de nos organisations administratives. Il en va de la capacité de la France à « rester dans la course » et, *in fine*, du succès de nos armes.

I. LES ARMÉES FRANÇAISES NE SONT PAS RESTÉES À L'ÉCART DE LA « RÉVOLUTION NUMÉRIQUE »

Les rapporteurs ont tenu à établir un bilan de la transformation digitale des armées au seuil de la période de programmation militaire 2019–2025. Il en ressort que les armées françaises sont loin d'être en retard dans l'appropriation des technologies numériques actuelles ; comme le dit l'amiral Arnaud Coustillière, futur directeur général du numérique du ministère des Armées, « *le ministère fait du numérique depuis très longtemps* » et ses responsables sont « *pleinement conscients du fait que ce domaine "explose", crée de la richesse, et modifie profondément les organisations du fait des gains d'efficience qu'il permet* ».

Le général Bruno Maurice, officier général chargé de la transformation digitale des armées auprès du major-général des armées, a expliqué que l'enjeu général de la transformation digitale se résume ainsi : « **gagner avec le digital** », non seulement dans le domaine opérationnel mais aussi dans le domaine dit « organique », c'est-à-dire l'environnement et du soutien des armées. Selon ses explications, la « transformation digitale » se définit comme « *la rencontre d'une rupture technologique avec de nouveaux usages, rendus possibles par la maîtrise de la donnée et de son traitement* ». Le changement des usages suppose en effet la disponibilité et la maîtrise des données ; pour être exploitées, les données doivent être normées et sécurisées. Pour le général Bruno Maurice, « *il s'agit donc d'abord d'un processus " métier", visant à créer de la valeur pour ses bénéficiaires : l'usager est au centre de la dynamique* ».

Le bilan de la numérisation des armées fait cependant apparaître un décalage d'avancement entre, d'une part, l'intégration des technologies numériques aux systèmes d'armes, déjà très poussée et, d'autre part, la numérisation de l'environnement et du soutien des forces, moins avancée.

A. LES SYSTÈMES D'ARMES SONT DÉJÀ LARGEMENT NUMÉRISÉS

Les systèmes d'armes intègrent les technologies numériques depuis plusieurs décennies déjà. Si les armées françaises possèdent ainsi des équipements « de pointe », qui n'accusent pas de retard marqué par rapport à l'état actuel des développements technologiques, c'est parce que la base industrielle et technologique de défense (BITD) française, faisant fond sur un écosystème de recherche très solide, a su prendre le tournant de la numérisation.

1. L'intégration du numérique aux systèmes d'armes est à l'œuvre depuis longtemps

Si les parcs d'équipements des armées sont parfois vus comme trop limités en volume ou constitués pour une part de matériels vieillissants, il faut reconnaître que, dans l'ensemble du spectre des matériels, la France dispose de systèmes

d'armes qui ne sont pas déclassés au regard de l'évolution technologique. Ce constat vaut autant pour les armes elles-mêmes que pour les réseaux qui permettent de les mettre en œuvre de façon coordonnée.

a. Des armes intégrant les technologies numériques avancées

L'ingénieure générale Caroline Laurent, directrice de la stratégie de la direction générale de l'armement (DGA), a estimé qu'aujourd'hui, les forces françaises disposent de systèmes numérisés à un niveau satisfaisant par rapport aux grandes nations occidentales, soulignant que l'enjeu réside pour elles dans les prochaines étapes de numérisation. Ce constat vaut pour l'ensemble des milieux d'opération des armées.

Ainsi, s'agissant par exemple du milieu maritime, l'amiral François Moreau, sous-chef d'état-major chargé des plans et des programmes de l'état-major de la marine nationale, a souligné que la numérisation n'est pas une nouveauté pour la marine, qui opère des systèmes numérisés « ***depuis trente ou quarante ans*** ». Notant « *une accélération récente* » dans cette tendance, il a fait valoir que la frégate multi-missions (FREMM) et la frégate de taille intermédiaire (FTI) peuvent être vues comme « *des bâtiments numériques* », et que l'environnement et le soutien de la flotte ont eux aussi été numérisés. Il a expliqué que « *l'approche de la marine nationale en matière de numérisation est* ***focalisée sur le combat*** », c'est-à-dire l'intérêt de la numérisation se mesure à ce qu'elle peut apporter comme capacité opérationnelle supplémentaire. Le constat est le même dans les autres armées.

b. Des systèmes performants de mise en réseau des forces

En plus de l'intégration de l'informatique aux armes elles-mêmes, la numérisation des systèmes d'armes passe par la mise en réseau des équipements. À cet égard également, les technologies employées par les armées françaises n'accusent pas aujourd'hui de retard – bien au contraire.

i. Des transmissions performantes

M. Marc Darmon, directeur général adjoint de Thales, a expliqué que les grands enjeux technologiques actuels concernant les télécommunications militaires des puissances occidentales portent sur l'augmentation de leurs débits, la garantie de leur résilience et de leur résistance, ainsi que sur la rapidité des communications – c'est-à-dire d'absence de latence –, afin de permettre le combat « collaboratif » et l'adaptation des matériels à des environnements « abrasifs » de toute nature.

En la matière, selon lui, **la France est « *à la pointe* »**, que ce soit en matière de radio logicielle ou de télécommunications spatiales protégées contre le brouillage. En effet, le brouillage des transmissions satellitaires constitue la principale des menaces pesant sur nos systèmes de communication, car nos hautes capacités de cryptage et de changements rapides de fréquences offrent un niveau

de sécurité déjà très satisfaisant pour nos transmissions par radio. L'industrie française s'impose ainsi comme une référence mondiale en matière de transmissions. À titre d'exemple, la radio PR4G est utilisée par 45 armées de terre au monde, et la radio Contact est encore plus performante.

ii. Une avance française dans l'info-valorisation du combat

L'état des capacités de nos armées en matière d'exploitation des données informatiques au cœur des forces au combat, couramment appelée « info-valorisation », au regard des technologies actuelles, est également favorable. Ainsi, pour prendre l'exemple de l'armée de terre, on relèvera que la numérisation des forces a commencé dès les années 1990 avec la mise en œuvre du concept de « **numérisation de l'espace de bataille** » (NEB).

Le général Bernard Barrera, sous-chef d'état-major de l'armée de terre chargé des plans et des programmes à la date de son audition et désormais major-général de l'armée de terre, a fait valoir qu'en dépit d'une architecture parfois rigide ou cloisonnée ainsi que de limites incontestables, la NEB a permis « *d'acculturer l'armée de terre à la numérisation depuis vingt ans* ». D'ailleurs, selon lui, elle a procuré « *un certain avantage opérationnel* », et c'est sur elle qu'est bâti le programme d'info-valorisation et de mise en réseau des véhicules de l'armée de terre dans le cadre d'une vaste opération appelée SCORPION [(1)] : « *SCORPION repose sur une logique de "super-NEB"* ».

C'est ainsi que, comme l'a dit le général Bernard Barrera, « ***la France va prendre de l'avance en matière de combat info-valorisé*** ». Britanniques et Américains n'en sont pas au même niveau d'ambition, et les Français sont seuls à préparer le **combat « collaboratif »**, c'est-à-dire le transfert de fichiers entre engins terrestres, la localisation des forces amies (*Blue Force Tracking*) et la radio bi-bande, le tout assurant le partage des informations en moins d'une seconde, à partir de 2025.

iii. Des « capteurs » particulièrement efficaces pour le renseignement

Le général Jean-François Ferlet, directeur du renseignement militaire (DRM), a jugé que le renseignement français dispose aujourd'hui de **capteurs performants**, avec un niveau technologique qu'il est d'ailleurs impératif de maintenir par des investissements suffisants compte tenu de la rapide évolution des technologies concernées, que nos adversaires ne manquent pas d'utiliser.

Notamment, les capacités françaises en matière de capteurs satellitaires optiques sont excellentes, avec les programmes Hélios puis MUSIS. Les Allemands et les Italiens se sont spécialisés dans les capteurs satellitaires radars, qui ont une capacité de surveillance par tout temps, et possèdent un spectre de détection différent de celui de l'optique. Une coopération a donc été mise en place par la France avec l'Allemagne et l'Italie, consistant en un système de droits de

(1) Synergie du contact renforcée par la polyvalence et l'info-valorisation.

tirage des trois États sur les équipements concernés de leurs partenaires, dans des conditions qui garantissent l'accès de chacun à des capacités performantes dans de bonnes conditions de confidentialité.

Globalement, qu'il s'agisse de renseignement d'origine « image » (ROIM), d'origine électromagnétique (ROEM) ou, de plus en plus, d'origine cyber (ROCyber), le directeur du renseignement militaire considère que « ***le niveau de performance des services est excellent*** ». Il fait d'ailleurs valoir qu'il y a de fortes synergies entre certains types de renseignement, « *par exemple entre le ROCyber et le ROEM lorsque l'on "capte" un* smartphone ».

iv. Une appropriation efficace des technologies de télécommunication : l'exemple d'Auxylium

Les rapporteurs se sont attachés à étudier un nouveau système de communications tactiques de l'armée de terre en détail avec son concepteur, le capitaine Jean-Baptiste Colas, officier de programme pour Auxylium et conseiller chargé de l'innovation auprès du délégué général à l'armement. Ce programme est en effet emblématique de l'appropriation rapide des technologies numériques par les armées.

Le système Auxylium repose sur **un téléphone du commerce relié à un poste radio** par *Bluetooth*. Cette architecture ressort de discussions avec les soldats, le recours à un poste radio étant nécessaire pour que les militaires accèdent à leurs propres réseaux de communication. Ce poste radio, appelé Helium, est « *le moins encombrant au monde* », fabriqué en France sous brevet de la DGA. Pour regrouper les deux réseaux sur un seul et même appareil, il aurait fallu modifier le *smartphone*, « *mais aucun industriel français ne propose ce service pour des smartphones "grand public"* ». En outre, cette architecture présente des avantages en matière de sécurité de communications, et articulant deux batteries au lieu d'une, elle permet de ménager l'autonomie du système. Par ailleurs, elle constitue en elle-même une source d'économies, car le *smartphone* doit être renouvelé tous les trois ans, tandis que le poste radio peut durer six ou sept ans. Un dispositif de double carte SIM ne remplirait pas les mêmes fonctions, car il faudrait une ou deux minutes pour passer d'un réseau à un autre, alors qu'Auxylium permet d'en exploiter en même temps réseaux civils et réseaux militaires.

Auxylium permet de transmettre des ordres certifiés, y compris des ordres de tir. Les utilisateurs du système se voient attribuer des « profils » qui ouvrent des droits d'information différents. Aujourd'hui, chaque chef de patrouille Sentinelle en Île-de-France est équipé de ce système ; Auxylium permet ainsi d'accéder à la géolocalisation de toutes les patrouilles Sentinelle en Île-de-France.

Pourquoi doter les soldats d'un téléphone professionnel plutôt que d'une application à installer sur leur téléphone personnel ? Le capitaine Jean-Baptiste Colas a fait valoir un risque juridique – qui serait responsable en cas d'instruction

non reçue ? – ainsi qu'un risque technologique : « *mettre Auxylium sur App Store, ce serait y donner accès à n'importe qui* ».

La société Atos garantit plus de 99 % de taux de disponibilité du matériel. Les données recueillies sont stockées en *cloud* et hébergées par Atos. Le recours à une infrastructure d'hébergement déjà existante était en effet une condition de rapidité de mise en œuvre du système Auxylium. Ses logiciels reçoivent quatre mises à jour par an, élaborées à partir de l'exploitation des données d'utilisation et de discussions permanentes avec ses utilisateurs.

2. Notre base industrielle et technologique de défense a été pionnière en matière de numérisation

a. L'industrie de défense française s'est approprié très tôt les technologies numériques

M. Éric Trappier, président du groupement des industries françaises aéronautiques et spatiales (GIFAS), a rappelé que la numérisation de la BITD a commencé dans les années 1990, notamment avec le logiciel de conception assistée par ordinateur CATIA, développé par le groupe Dassault en vue de modéliser les produits industriels. Il a décrit les étapes successives de la numérisation de l'industrie de défense.

Dans un premier temps, celle-ci a concerné les plans des produits industriels, d'abord avec des systèmes de **maquette numérique** – Dassault étant le premier industriel à en maîtriser la technologie, suivi de Boeing. À partir de ces développements, la production elle-même a pu être organisée à partir de maquettes numériques. L'exploitation de celles-ci a permis de développer les techniques de **simulation du fonctionnement des matériels**, connues sous le nom de *Product Life Management*. Dans un second temps, les progrès de l'informatique ont permis de constituer des bases de données étendues – concernant par exemple les achats ou les composants technologiques – et d'exploiter celles-ci avec une puissance de calcul de plus en plus importante. Puis, la **fusion des différentes bases de données** a ouvert la voie à ce que M. Éric Trappier a appelé « *l'industriel entièrement numérisé* ». A suivi le développement de « **plateaux virtuels** », qui consistent à mettre en réseau l'ensemble des industriels partenaires d'un programme par l'interconnexion de leurs bases de données.

M. Stéphane Mayer, président du groupement des industries de défense et de sécurité terrestres et aéroterrestres (GICAT), a souligné que, dans le secteur de l'armement terrestre également, la numérisation de l'industrie est à l'œuvre depuis plusieurs années. Il a ajouté qu'aujourd'hui, **la réalité virtuelle** permet d'aller plus loin encore, en plaçant un équipage aux commandes d'un appareil en conception, dans une maquette numérique. Il en résulte des gains de temps et de coûts de développement.

Pour les grands industriels, l'enjeu est aussi de faire **accéder les « petits » industriels à ces technologies**. Le GIFAS a ainsi créé *Boost AeroSpace*, une plateforme numérique accessible aux petites et moyennes entreprises (PME) et aux entreprises de taille intermédiaire (ETI), « *pour lesquelles la numérisation est une condition de survie* ».

S'agissant de l'industrie de construction navale, les représentants du groupement des industries de construction et activités navales (GICAN) ont fait valoir que les progrès des technologies numériques dans l'industrie civile ont pu « *doper le numérique militaire* ». Pour le GICAN, il reste une certaine hétérogénéité dans l'appropriation du numérique : certains grands donneurs d'ordres sont déjà pleinement « *passés au numérique* », mais pour exploiter pleinement les possibilités du numérique, **il faut que l'ensemble de la *supply chain* atteigne le même niveau de compétence**. À cette fin, le GICAN met en œuvre, en partenariat avec *Boost Industrie*, divers projets de transformation numérique de toute la filière, concernant par exemple le développement de standards pour les maquettes numériques, les technologies de « jumeau numérique » des navires – qui consistent à élaborer une maquette numérique suffisamment complète pour pouvoir y simuler diverses opérations –, l'optimisation des opérations de maintenance en fonction de la disponibilité des chantiers, ou celle du démantèlement des navires.

b. La recherche numérique française est reconnue pour son excellence

De l'avis général, la France forme et accueille d'excellents chercheurs dans l'ensemble des domaines scientifiques sur lesquels les développements récents des technologies numériques ont fait fond, notamment les mathématiques, l'informatique, la physique ou la robotique.

S'agissant de la production de logiciels, l'Institut national de la recherche informatique et en automatique (INRIA), que présente l'encadré ci-après, est particulièrement reconnu pour son excellence.

L'Institut national de la recherche informatique et en automatique

Selon les explications de M. Antoine Petit, directeur général de l'INRIA à la date de son audition et désormais président du centre national de la recherche scientifique (CNRS), et Mme Isabelle Ryl, directrice du centre de l'INRIA à Paris, l'Institut a été créée sous le nom d'Institut de recherche en informatique et en automatique (IRIA) en 1967, dans le cadre du « Plan calcul ». M. Antoine Petit a rappelé que ce plan avait été élaboré par le Gouvernement en réponse au refus que lui avait opposé celui des États-Unis de vendre à la France le modèle d'ordinateur le plus puissant dont disposaient alors les Américains.

Depuis cette époque, l'INRIA est le seul établissement public à caractère scientifique et technologique à être placé sous la double tutelle des ministères de la Recherche et de l'Industrie, d'où des liens étroits et historiques avec l'industrie.

L'activité de l'Institut, du point de vue disciplinaire, relève de l'informatique et des mathématiques appliquées.

Il compte 2 600 chercheurs, dont un tiers seulement à statut permanent. Autre particularité, l'INRIA emploie des chercheurs de 106 nationalités différentes.

Le niveau d'excellence de l'INRIA est attesté par son attractivité pour les chercheurs, ainsi que par le nombre de bourses attribuées aux chercheurs de l'INRIA par le Conseil européen de la recherche (*European Resarch Council*, ERC). Ce régime de bourses individuelles offre des allocations de 250 000 à 500 000 euros par an ; chère, cette distinction est par nature rare, et le nombre de boursiers ERC ainsi que leur taux dans les effectifs place l'INRIA au premier rang européen d'excellence dans ses disciplines.

Pour M. Axel Legay, directeur adjoint du centre de l'INRIA à Rennes, la France « *n'a pas à avoir honte de ses capacités scientifiques* », qui sont, « *en niveau, tout à fait comparables à celles des Américains* ». C'est dans le montant des moyens investis qu'apparaissent d'importants écarts, mais pas dans la qualité des chercheurs. Les représentants de *Facebook* ont d'ailleurs souligné la **qualité des chercheurs français en matière d'intelligence artificielle**. Le responsable mondial de *Facebook* pour cette activité est un Français, M. Yann Le Cun, et Paris accueille le seul centre de recherche en matière d'intelligence artificielle qu'a créé *Facebook* en dehors de l'Amérique du Nord. *Facebook* a d'ailleurs noué avec l'INRIA un partenariat mutuellement avantageux, offrant un accès à ses calculateurs aux chercheurs de l'Institut.

B. LA NUMÉRISATION DES FONCTIONS « ORGANIQUES » ET DU SOUTIEN DES FORCES EST À L'ŒUVRE, AVEC UN SUCCÈS INÉGAL

Si les armées n'ont pas manqué d'informatiser leurs fonctions « organiques », l'échec de la numérisation du paiement de la solde demeure dans tous les esprits, et l'on attend beaucoup des chantiers de transformation numérique des différents services de soutien, d'administration et de gestion des armées.

1. Des systèmes d'information ont été développés dans l'environnement et du soutien des forces

M. Paul Serre, adjoint au secrétaire général pour l'administration (SGA) du ministère des Armées, a fait valoir qu'en matière d'administration et de gestion, le ministère ne pouvait pas échapper à la « révolution numérique » pour trois raisons :

– la numérisation est une **tendance lourde, traversant la société** et en particulier l'État, avec un important chantier numérique au sein du programme « Action Publique 2022 » ;

– les personnels du ministère sont « *des hommes et des femmes de leur temps* », et le ministère se doit d'être d'autant plus en accord avec les mœurs de l'époque que ses agents sont plus jeunes et plus souvent contractuels que la moyenne : ainsi, **la numérisation des services qui assurent leur soutien participe de l'attractivité des armées** et contribue *ipso facto* à fidéliser les militaires ;

– les agents des services de soutien eux-mêmes sont demandeurs **d'horizontalité**, de modes de travail nouveaux, d'évolutivité de leurs outils, toutes choses qui sont le nouveau *modus vivendi* des métiers concernés.

a. Le développement des systèmes d'information d'administration et de gestion et des systèmes d'information « métier »

i. Un vaste éventail de systèmes d'information

M. Paul Serre a expliqué que les systèmes d'information d'administration et de gestion (SIAG) comprennent aujourd'hui environ **650 applications informatiques**, parmi lesquelles 550 sont aujourd'hui en service et une trentaine constitue des « *projets à fort enjeu* ».

La majorité des 650 applications voit son développement externalisé, mais la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), opérateur du ministère, possède encore des centres de développement chargés de développer, en interne, des systèmes simples.

Depuis 2010, les SIAG font l'objet de 120 à 130 millions d'euros d'investissement par an. 40 % de cet investissement est consacré aux SIAG des ressources humaines. M. Paul Serre en a présenté plusieurs chantiers majeurs :

– la **gestion prévisionnelle des emplois et des compétences**, pour laquelle une base de données des métiers du ministère a été établie ; elle évoluera pour intégrer des outils de gestion prévisionnelle des compétences, sur la base des 32 familles professionnelles et des 150 filières identifiées par le référentiel des emplois et métiers du ministère. Le niveau de « granularité » de ce système va jusqu'à l'individu ;

– **Source Solde**, destiné à remplacer le calculateur de Louvois et celui de l'armée de l'air pour le calcul des soldes militaires. Le projet Source se décline aussi en un logiciel de gestion dématérialisée des pièces justificatives, ainsi qu'en « Source Web », interface unifiée qui sert à relier entre eux les systèmes d'information des ressources humaines et à fiabiliser leurs données ;

– **Alliance**, qui sert à la paie des personnels civils et évolue pour devenir « Alliance NG » ;

– une **offre digitale de services dans le domaine de l'action sociale**, avec une plateforme « *ergonomique et intuitive* », qui permettra à terme aux personnels du ministère des Armées et à leurs familles de formuler les demandes d'aides et de prestations sociales de façon plus simple qu'aujourd'hui.

Ces systèmes intègrent un service : le **suivi de la situation des administrés par eux-mêmes sur internet**. Certaines données seront ainsi saisies *via* l'intranet mais consultables sur internet.

La constitution d'une base de données de gestion des habilitations constitue un autre enjeu de la transformation numérique du ministère des Armées. Ce chantier fait partie du projet **Défense Plateforme**, « *très structurant* » car il « *constitue le socle de l'outil numérique* » du ministère. Ouverture des données et interfaçage entre intranet et internet en sont les principaux aspects. Des expérimentations sont d'ores et déjà en cours.

Les 60 % restants des investissements annuels en SIAG portent sur les soutiens présentant un caractère plus logistique, ou sur des sujets d'intérêt commun tels que la messagerie électronique ou la signature électronique. En outre, dans le domaine des **achats** – qui représente, hors armement, quatre milliards d'euros par an –, un nouveau système appelé **Alpha** est en cours de déploiement pour **dématérialiser l'ensemble du processus d'acquisition**.

Un des sujets de compétence propre du SGA, le lien armées-jeunesse, a la spécificité de conférer au SGA des liens avec des usagers externes, à savoir 800 000 jeunes par an. « **majdc.fr** », à la fois site internet et application pour *smartphone*, sert à établir un « pont » avec les cohortes des jeunes et vise à « *faire vivre* » le lien entre armées et jeunesse. Il permet aux jeunes Français de conserver les supports d'enseignement de la journée de défense et de citoyenneté, d'en recevoir des mises à jour, « *de façon à ce que la journée "défense et citoyenneté" ne soit pas sans lendemain* ».

ii. Un échec sapant la confiance dans les systèmes d'information : Louvois

Lors de leurs déplacements, les rapporteurs ont pu constater que les dysfonctionnements graves et répétés du système de calcul de la solde appelé Louvois [(1)] pouvaient susciter chez les militaires une certaine méfiance envers les grands projets de systèmes d'information. L'encadré ci-après présente une analyse « à froid » des causes de ces dysfonctionnements. M. Paul Serre a assuré les rapporteurs que des leçons avaient été tirées de Louvois en matière de conduite de projet, ce qui a amené à confier la direction du projet Source Solde à la DGA, dont les compétences en matière de gestion de projets complexes sont reconnues.

Les raisons de l'échec de Louvois

● Selon M. Paul Serre, « *la **cartographie des responsabilités** au sein du ministère n'était pas bonne* ». Louvois remplaçait des systèmes de moindre périmètre, gérés par des **règles souvent non écrites**, connues par les « soldiers ». La contrainte de déflation des effectifs, concomitante avec le déploiement de Louvois, a conduit certains responsables à supprimer plus rapidement que de raison les postes de « soldiers ».

● « ***Tout est-il vraiment informatisable ?*** » Ce n'est pas certain dans un système aussi complexe que la solde des personnels.

● Le calculateur Louvois n° 3 était le fruit d'un **développement interne, avec des fonctionnalités mal codées, donc instables**. La régularisation *a posteriori* fonctionnait mal, alors que la solde repose beaucoup sur des systèmes d'avances régularisées par la suite. De

(1) Logiciel unique à vocation interarmées de la solde.

ce fait, « *concrètement, la même équation ne donne pas toujours la même solution dans le calculateur Louvois* ».

● Face aux premiers dysfonctionnements, on avait choisi de **déverrouiller certaines des sécurités** de Louvois pour « forcer » des versements, ce qui a achevé de rendre le système défaillant, celui-ci n'étant plus capable de juger de la cohérence des versements dus ou indus.

Ainsi, « *négligence de la compétence humaine, "rafistolages risqués" d'un logiciel défectueux et manque de répartition claire des responsabilités, voilà les causes de l'échec de Louvois* ». On notera d'ailleurs que personne n'a été sanctionné, ce qui est certainement le signe du caractère collectif des responsabilités.

Pourquoi le logiciel de comptabilité Chorus a-t-il fonctionné, et pas Louvois ? À partir de 2010, Chorus a remplacé onze applications du ministère et a permis d'en supprimer une vingtaine. Le ministère de la Défense a été pionnier dans ce projet, et le chantier a été conduit dans les temps… « *mais pas sans peine* », a précisé M. Paul Serre. « *Bercy a dû gérer un goulet d'étranglement* », ce qui a conduit à déconcentrer certaines responsabilités aux ministères ; de plus, le transfert des données ne s'est bien sûr pas fait sans erreurs, « *avec des conséquences lourdes pour les paiements* ». Mais « *dans l'ensemble, le basculement vers Chorus s'est fait sans trop de difficultés* », et a permis de professionnaliser ainsi que de rationaliser la gestion financière du ministère. À titre d'exemple, le délai de paiement moyen a été divisé par deux, à 22,3 jours.

b. Une « urbanisation » encore incomplète

D'après l'amiral Arnaud Coustillière, **reste à améliorer l'« urbanisation » des systèmes d'information** – c'est-à-dire la cartographie qui définit des « pavés fonctionnels » pour chaque système et des mesures visant à assurer la cohérence des systèmes qui doivent être interconnectés. Selon l'amiral, la sphère des ressources humaines est « *très mature de ce point de vue* » ; tel est moins le cas, par exemple, de celle de la maintenance.

La direction générale des systèmes d'information et de communication (DGSIC) – dont la transformation a été annoncée en « direction générale du numérique » (DGNUM) – « *ne fait pas le travail des directions fonctionnelles à leur place* », mais est chargée d'évaluer leur degré de maturité en matière d'urbanisation des systèmes. En outre, selon M. Paul Serre, la maîtrise du cœur des API [(1)] et des bases de données est l'objet d'un travail conjoint avec la DGNUM, précisant qu'en la matière, « *l'essentiel du travail reste à faire* ». Et encore, a fait valoir le colonel Olivier Kempf, chargé de mission pour la transformation digitale à l'état-major de l'armée de terre, l'interconnexion des systèmes d'information par API n'est pas toujours fonctionnelle compte tenu de l'âge et de la configuration des systèmes.

(1) Application Programming Interface *(interface de programmation applicative), outil informatique servant de « raccord » entre deux bases de données.*

D'après le général Bernard Barrera, cette configuration s'explique principalement par **l'histoire des systèmes d'information**, qui ont été développés suivant une logique « métier » et « *top–down* », très contradictoire avec les besoins d'utilisation transverse des opérateurs de terrains. C'est pourquoi, aujourd'hui, le paysage des systèmes d'information dans chaque armée ressemble aujourd'hui « *à un plat de spaghetti* », selon l'expression d'un militaire. Un régiment doit en effet opérer **une trentaine de systèmes** d'information.

Pourtant, en la matière, un certain degré de transversalité dans les systèmes d'information est particulièrement nécessaire aux échelons bas de commandement, pour rationaliser la charge de saisie informatique. En effet, comme l'a souligné le colonel Olivier Kempf, il en va de la fiabilité des données : si l'on se contente de fusionner les données de plusieurs systèmes par un dispositif automatisé – aussi perfectionné soit-il –, **plus il y a d'opérations de saisie sur le terrain, plus il y a de risques d'erreurs**.

2. Le ministère des Armées a entamé une ambitieuse démarche de « transformation numérique »

a. « Le numérique » fait l'objet d'un pilotage renforcé

i. Une autorité stratégique pour les systèmes d'information et les données

L'amiral Arnaud Coustillière a présenté le champ de compétences et la place de la direction générale des systèmes d'information et de communication – future DGNUM – au sein du ministère en expliquant au préalable que :

– **la cyberdéfense est à ses yeux indissociable de la transformation digitale**, dont elle assure la sécurité et dont elle se nourrit ;

– la stratégie gouvernementale « Action publique 2022 » met l'accent sur **la numérisation comme levier de réforme de l'État** et, signe de l'importance de ces chantiers, le secrétariat d'État au numérique est rattaché directement à Matignon.

Lors d'un comité exécutif (COMEX) de 2017, a été décidé un « *nouveau positionnement* » de la future DGNUM, qui aura une double mission :

– une « ***mission classique de direction générale des systèmes d'information et de communication (DSI) de groupe*** », rattachée au COMEX et dotée d'une autorité fonctionnelle plus ou moins forte sur les DSI des « entités du groupe » (en l'espèce, les armées, directions et services du ministère) ;

– une « ***mission nouvelle de "chef d'orchestre" de la transformation numérique*** » du ministère. Dans ce cadre, la DGNUM aura pour mission de créer « *un environnement stimulant* » pour les projets de transformation numérique, qui « *ne peuvent par nature être efficacement portés que par les "métiers"* ». En

accompagnement de cette mission, la ministre des Armées a nommé le directeur général « administrateur ministériel des données ».

L'amiral Arnaud Coustillière a précisé que s'agissant de la numérisation du champ de bataille, la DGNUM se bornera pour l'essentiel à travailler à l'ouverture des données, à la cohérence de l'urbanisation des systèmes d'information, et à veiller à la cohérence des technologies employées, car « *elle n'a aucune plus-value dans les discussions entre la direction générale de l'armement et l'état-major des armées* ». Pour lui, « *une DSI de groupe doit apporter de la plus-value aux "métiers" et traiter les affaires transverses* ».

Comme la DGSIC actuelle, la DGNUM comptera quelques dizaines d'agents et, rattachée directement à la ministre, elle aura « ***une autorité de niveau stratégique*** » pour « *garantir à la ministre la cohérence de son système d'information* ».

À cet effet, un conseil des systèmes d'information et de communication se réunit déjà tous les six mois pour arrêter des orientations. Le DGSIC en coordonne la mise en œuvre en réunissant régulièrement les responsables des systèmes d'information de l'état-major des armées, de la DGA, du SGA et de la DIRISI.

ii. Un opérateur historique

La DIRISI est **l'opérateur de référence** du ministère des Armées. Son pilotage, assuré de façon « *partagée entre la DGSIC et l'état-major des armées* » est en cours de renforcement « *au travers de règles de bonne gouvernance, du fait de la complexité croissante du numérique et de son extension* ».

Elle est placée sous l'autorité hiérarchique du CEMA « *et doit le rester* » car elle est « *essentielle aux opérations militaires* », mais elle a aussi une mission dans un champ plus large, lié au bon fonctionnement du ministère : elle opère les réseaux de communication militaires en OPEX (comme Syracuse), tout en gérant certains grands réseaux pour l'ensemble du ministère (tel Intradef). D'autres services sont opérateurs de leurs propres réseaux, à l'image du service de santé des armées, mais œuvrent en lien étroit avec la DIRISI.

b. La transformation digitale des armées est érigée en priorité

Le rapport annexé au projet de loi de programmation militaire pour les années 2019 à 2025 érige la transformation digitale en priorité pour l'action du ministère. Il la présente comme « *une démarche volontaire visant à s'approprier au plus vite et dans les meilleures conditions les technologies émergentes* », afin de « ***générer des évolutions significatives dans les usages et les modes de travail*** ». Le rapport annexé explique que l'exploitation des données numériques permettra de « *transformer les organisations et les domaines d'emploi* ». Il fixe à cette transformation trois objectifs :

– garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations ;

– renforcer **l'efficience des soutiens et faciliter le quotidien** du personnel ;

– améliorer la **relation au citoyen et aux personnels** ainsi que **l'attractivité** du ministère.

II. LES RUPTURES TECHNOLOGIQUES À VENIR DANS LE NUMÉRIQUE PEUVENT ACCROÎTRE LA PERFORMANCE DE NOS ARMÉES MOYENNANT DES INVESTISSEMENTS SUPPLÉMENTAIRES

Sans prétendre disposer de toutes les compétences nécessaires pour établir des prévisions précises d'évolution des technologies – prophéties qui, même faites par des techniciens, s'avèrent d'ailleurs souvent hasardeuses –, les rapporteurs se sont attachés à étudier les voies de recherche et de développement (R&D) généralement considérées comme les plus prometteuses et porteuses des plus grands changements pour les armées. Il en ressort que les ruptures technologiques à venir sont de nature à modifier profondément nos armées, tant dans le champ opérationnel qu'en matière « organique ».

Relever ces défis suppose de consentir des investissements, mais permettra à nos armées, en retour, de gagner en efficacité en opération et en efficience « organique ». Mais relever les défis de la « révolution numérique » n'est possible qu'en prenant appui sur un solide écosystème de recherche et d'innovation.

A. LA « RÉVOLUTION NUMÉRIQUE » EST APPELÉE À SE TRADUIRE PAR DE NOUVELLES RUPTURES TECHNOLOGIQUES

Les rapporteurs ont retenu huit principaux champs dans lesquels, de l'avis général, des ruptures technologiques sont envisageables : le *big data*, la fabrication additive – ou « impression en trois dimensions » (3D) –, le calcul intensif, l'intelligence artificielle, la robotique et les drones, l'informatique quantique, les applications futures de la convergence – à l'œuvre aujourd'hui – entre les neurosciences et le numérique, et l'internet des objets.

1. Le traitement du *big data*

On entend par *big data* les techniques permettant d'exploiter des masses de données si volumineuses que les besoins de leur traitement dépassent les capacités humaines ainsi que celles des systèmes classiques de gestion des bases de données.

a. Traiter un « déluge d'informations »

La « révolution numérique » se traduit, par nature, par une **production exponentielle de données**. Une étude de la *Dwight D. Eisenhower School for National Security and Resource Strategy* (1) présentée aux rapporteurs par l'attaché d'armement près l'ambassade de France aux États-Unis donne une mesure de cette croissance : 90 % des données existantes dans le monde ont été produites dans les

*(1) Nouvelle appellation de l'*Industrial College of the Armed Forces*, que l'on pourrait comparer à la session « armement et économie de défense » de l'institut des hautes études de la défense nationale (IHEDN).*

deux dernières années, et le volume total de ces données a été multiplié par cinquante de 2010 à 2017.

Le traitement de ces masses d'information dépasse les capacités des bases de données classiques et nécessite des algorithmes particulièrement performants pour en assurer **le traitement, le filtrage et le partage**.

M. Patrick Pailloux, directeur technique de la direction générale de la sécurité extérieure (DGSE), a expliqué que les armées et les services de renseignement utilisent, pour le tri des données, des algorithmes de ciblage plus précis que ne le permettent les applications civiles, par exemple celles de l'industrie publicitaire. Pour surveiller, par exemple, les connexions et communications entre des cibles d'intérêt dont les liens ne sont pas connus à l'avance, les moyens humains ne suffiraient pas. Mais en tout état de cause, si un algorithme met en évidence une information utile, celle-ci doit toujours être vérifiée. De même, le général Jean-François Ferlet a souligné que si la direction du renseignement militaire, qu'il commande, dispose de capteurs performants, **le principal enjeu pour la performance du renseignement tient non aux capacités de recueil de données, mais aux capacités d'exploitation de ces données**. En effet, « *il ne suffit pas qu'un individu soit répertorié dans une base de données ; encore faut-il exploiter les données pour produire un renseignement véritablement utile* ». Or le « déluge informationnel » croissant ne pourra plus être traité exclusivement par les moyens essentiellement humains qui prévalent aujourd'hui.

L'étude précitée de l'*Eisenhower School* voit dans le *big data* **la « *nouvelle frontière* » des technologies de l'information**. La maîtrise de ses applications suppose que les technologies prennent en compte les enjeux dits des « 5 V » :

– volume d'information croissant, qui suppose des capacités de transport et de traitement des données ainsi qu'une certaine standardisation de leurs formats ;

– rapidité (*velocity*) dans la circulation de l'information ;

– diversité (*variety*) des sources et des prismes d'analyse ;

– véracité (*veracity*) des informations ;

– intérêt intrinsèque (*value*) des informations, qui doivent être hiérarchisées en fonction des besoins de leur récepteur.

b. De multiples applications possibles pour le renseignement, les opérations ou le soutien des forces

Sans prétendre à l'exhaustivité, les rapporteurs se sont attachés à étudier les applications possibles du *big data* dans les armées.

i. Des applications dans le domaine du renseignement

Le directeur du renseignement militaire a expliqué que, d'ores et déjà, **des briques de systèmes d'information ont été construites pour analyser les données** produites par les « capteurs » des services de renseignement. Par exemple, un logiciel permet de vérifier si une image comporte un élément non naturel. De même, la DGSE a développé un outil appelé TIM (pour « traitement de l'information magnétique »), qui est aujourd'hui en cours de déploiement au sein des autres services et des unités des Armées.

Les services visent cependant à développer un **outil plus global**. En effet, les bases de données des différents services comportent des **données de natures très hétérogènes** – sons, images, pages *Facebook*, éléments biométriques collectés en OPEX, etc. –, qui doivent être « formatées » pour pouvoir être exploitées par les mêmes outils.

Or le ***big data*** permet d'aller beaucoup plus loin dans les activités de renseignement qu'une simple requête faite par un opérateur dans un moteur de recherche sur la base d'étiquetages des données – par exemple en cherchant un nom propre précis dans une base de données spécifique. Dans cette optique, la DGA conduit un programme d'architecture de traitement et d'exploitation massive de l'information multi-source (**ARTEMIS**), que le directeur du renseignement militaire a décrit comme une sorte de « système de systèmes », qui vise à exploiter des bases de données de toutes natures.

ii. Des applications dans le domaine de la planification et de la conduite des opérations

Non seulement, au niveau stratégique, on prévoit une forte croissance du volume d'informations produites par les systèmes de renseignement et utilisées pour la planification et la conduite des opérations, mais au niveau tactique, les systèmes d'armes eux-mêmes sont dotés de capteurs de plus en plus performants. Il en résulte le même phénomène de « déluge d'information ».

Pour tirer le meilleur parti de ces informations aux niveaux tactique et opératif, les équipements devront être dotés de systèmes de *big data*.

Tel est le cas, par exemple, avec le « centre opérationnel du futur » développé par Naval Group pour les navires de surface, que les rapporteurs se sont fait présenter lors de leur déplacement à Ollioules, dans le Var, sur un site de R&D de Naval Group. L'enjeu de ce développement tient à la **conciliation de deux tendances en premier lieu contradictoires** pour l'architecture des centres opérationnels des navires : d'une part, une **exigence de simplicité d'utilisation** des outils par les marins ; d'autre part, la complexité croissante des systèmes d'armes et le « **déluge informationnel** » résultant de leur numérisation. L'interface homme–machine repose sur une dalle tactile comparable, par ses modalités d'usage, avec celles fournies par l'industrie civile ; elle présente une grande variété de données de façon agrégée, parfois en trois dimensions.

iii. Des applications dans le domaine « organique »

Les développements récents des technologies permettent d'envisager de doter les matériels militaires de capteurs d'auto-diagnostic.

Ainsi, le président du GICAT a indiqué que l'industrie d'armement terrestre commence à pouvoir **simuler les opérations de maintenance**, l'opérateur évoluant dans une maquette virtuelle. Surtout, avec les équipements de la génération SCORPION, la **maintenance prédictive** permettra d'optimiser les stocks et, selon lui, de prévoir les pannes dans nombre de cas. Pour ce faire, les systèmes en question exploiteront les données de maintenance par des techniques de *big data*.

Autre exemple d'application du *big data* à l'entretien des équipements, les ingénieurs de Naval Group à Ollioules ont présenté aux rapporteurs un projet de maintenance informatisée des navires, appelé « i-maintenance ».

Il repose sur un **centre opérationnel de soutien intégré numérique**, construit sur fonds propres en 2017 à Toulon. Il s'agit d'un « data center *à la pointe de la technologie* », doté d'une « *capacité de stockage monumentale* », dans lequel Naval Group vise à exploiter les masses de données relatives à l'état des navires par des technologies de *big data* et d'intelligence artificielle, afin d'optimiser la maintenance des bâtiments. C'est aussi depuis ce centre qu'un système de visioconférence permet à l'équipage de dialoguer avec l'industriel à des fins de téléassistance. Avec la numérisation d'une part croissante des équipements des navires, les services de maintenance pourront en effet s'appuyer sur l'informatique pour diagnostiquer les pannes et en traiter certaines par des correctifs informatiques. L'encadré ci-après présente ce projet, dont le principe vient de faire l'objet d'une étude technico-opérationnelle lancée par la DGA.

Les possibilités ouvertes par le *big data* en matière de maintenance : l'exemple du projet « i-maintenance » de Naval Group

En cas de panne, le système vérifie qu'il ne s'agit pas d'une fausse alerte en mettant en œuvre des tests des capteurs. Depuis février 2018, Naval Group est en mesure de déployer des puces spécifiques sur les pièces d'un navire, comportant un lien automatique vers la documentation technique pertinente. Pour les navires nouveaux, cette documentation est d'emblée numérique ; pour les navires anciens, la marine et l'industriel reconstruisent *a posteriori* les données nécessaires.

Naval Group peut également équiper les navires de composants qui collectent des données, lesquelles peuvent être transmises à terre comme à l'équipage pour les besoins de la maintenance. Ces informations permettent, en cas de panne, d'analyser les causes de la dérive en reconstituant l'incident ; il s'agit là de techniques de modélisation. Si la panne ne peut pas être diagnostiquée à bord, des technologies de *big data* permettent d'opérer des analyses depuis la terre pour corréler les « symptômes » de la panne avec ce qui est advenu sur d'autres navires afin de proposer un diagnostic ainsi qu'une procédure de réparation ou de restauration des fonctions, éventuellement avec des performances dégradées.

L'équipement en puces RFID et en capteurs sert aussi à accroître la productivité des visites des bateaux à quai, en informatisant les relevés d'informations. Les données ainsi

collectées sont ensuite capitalisées dans le *data center* de Toulon. Ainsi, « *on saura qui a posé quel boulon, quand et pourquoi* ».

iv. Des implications pour les procédures de commandement et de contrôle des opérations

Comme l'a expliqué M. Gérard de Boisboissel, secrétaire général de la chaire de cyberdéfense et de cybersécurité de Saint-Cyr, « ***le "tout-numérique" bouleverse la façon d'opérer*** ». En effet, avec la précision croissante des capteurs et le perfectionnement des transmissions numériques, les technologies nouvelles permettent quasiment « *au général voire au Président de la République de regarder par-dessus l'épaule du chef tactique* ».

Ces technologies de traitement et de transmission de l'information en masse modifient ainsi l'équilibre des responsabilités dans la chaîne de commandement, voire la notion même de subsidiarité. À ce titre, elles nécessitent des études doctrinales approfondies sur les responsabilités de chaque échelon hiérachique.

2. La fabrication additive

Lors de leur déplacement aux États-Unis, les rapporteurs se sont fait présenter, au Pentagone, les progrès et le potentiel de la fabrication additive par le colonel Howard Marotto, directeur adjoint du service de la logistique de nouvelle génération en charge de l'innovation et de la fabrication additive à l'état-major du corps des *Marines*.

a. Les progrès récents et prévisibles en matière de fabrication additive

Le développement des techniques d'impression 3D permet aujourd'hui de fabriquer des pièces tout à fait solides. Selon le colonel Howard Marotto, certaines résines produites par la société israélienne Ultem permettent d'imprimer des pièces aussi résistantes et plus légères que l'aluminium. Signe selon lui de cette fiabilité, 60 % des pièces (représentant 40 % du poids) de la prochaine génération de lanceurs spatiaux de SpaceX seront fabriquées à de façon additive, ce choix répondant à la fois à des objectifs d'optimisation de l'usage des matières premières et de contrôle de la *supply chain*.

Les progrès récents dans les technologies de fabrication additive ont donné lieu à diverses annonces, certaines restant à vérifier – comme, par exemple, l'annonce de la construction d'une maison entière par impression 3D en Chine. En tout état de cause, la maîtrise de la **fabrication métallique** par impression 3D progresse, ce qui permet d'« imprimer » aujourd'hui des véhicules, et le cas échéant des drones. De plus, la **fabrication additive d'éléments en béton** est envisageable à moyen terme ; elle intéresse d'ailleurs la NASA.

Les tests faits par les *Marines* montrent que la fabrication additive est possible même à bord des navires, où les vibrations des bateaux se sont même avérées avoir pour effet de rendre les polymères plus robustes.

b. Une « nouvelle révolution industrielle » ?

Le colonel Howard Marotto a présenté la fabrication additive comme « *une nouvelle révolution industrielle* » qui se caractérise par :

– la **réversibilité des outils de production** : une même imprimante 3D peut servir à produire différents matériels, sans distinction de gamme industrielle. Ainsi, pour les armées, elle ouvre la voie à des possibilités accrues de **coopération** en matière d'armement : une machine américaine pourrait imprimer des matériels français, et inversement ;

– **un déplacement de la valeur ajoutée, qui réside davantage dans les plans** d'un matériel que dans les capacités de production. Un tel déplacement serait de nature à modifier les rapports de forces entre puissances industrielles, au bénéfice d'États qui ont conservé d'importantes capacités d'ingénierie mais ont perdu une large part de leurs capacités de production. En outre, les relations entre les forces armées et leurs fournisseurs industriels sont appelées à changer, dès lors que les forces elles-mêmes possèdent des capacités de fabrication. Un modèle possible de contractualisation peut alors reposer sur le versement, à chaque impression d'un matériel, d'une redevance forfaitaire à l'industriel qui l'a conçu ;

– un **nivellement des capacités de production** : avec l'impression 3D, la production d'armes devient accessible à davantage d'États, voire d'acteurs non-étatiques. Le colonel Howard Marotto a fait valoir qu'à cet égard, de façon paradoxale, les développements technologiques ont pour effet que **c'est sur les hommes et les femmes, notamment les chefs tactiques, que repose de plus en plus l'ascendant opérationnel**. En effet, dès lors que la supériorité technologique de l'Occident est érodée par cette tendance au nivellement, la supériorité opérationnelle dépend de l'usage que chaque partie réussit à faire des technologies disponibles. Or, à ses yeux, les Occidentaux disposent en la matière d'un avantage : « *la liberté de penser est un facteur d'innovation* », qu'il faut exploiter.

c. La feuille de route des* Marines *pour l'appropriation des technologies de fabrication additive

Il ressort des travaux des services du colonel Howard Marotto que l'appropriation des technologies de fabrication additive par une force armée peut judicieusement suivre le processus suivant :

– d'abord, « ***commencer "petit"*** », en déployant un dispositif de fabrication additive sur un théâtre ;

– ensuite, favoriser l'emploi de l'impression 3D pour la **réparation de pièces simples**, produites en matière plastique ;

– dans un troisième temps seulement, étendre le recours à la fabrication additive à la **production de pièces métalliques, plus grandes et plus complexes**, ce qui permet de réduire le volume et l'« empreinte » de la logistique et de la *supply chain* industrielle, notamment en opération ;

– **enfin, généraliser la fabrication additive pour la réparation** de pièces en OPEX à chaque fois que la technologie le permet, même si c'est pour ne produire que des palliatifs provisoires permettant d'attendre la fourniture de pièces usinées classiques, qui est souvent soumise à de longs délais logistiques.

d. Les avantages de la fabrication additive

Le colonel Howard Marotto a expliqué que pour le corps de *Marines*, la fabrication additive présente les intérêts suivants :

– elle permet de fabriquer **non seulement des pièces détachées de tous types, mais aussi des armes**. Les *Marines* ont testé avec succès l'impression 3D de la totalité d'un système de lance-grenades, munitions comprises ; ils ont également réussi à imprimer un système autonome terrestre. Non seulement la fabrication de l'arme est techniquement possible, mais de surcroît, l'arme imprimée en 3D peut être plus précise que la même arme fabriquée de façon traditionnelle. Le colonel Howard Marotto a présenté aux rapporteurs le cas d'un mortier et de sa munition, dont l'impression 3D permet de maîtriser le processus de fragmentation et donc de « *moduler "sur-mesure" la létalité* » ;

– elle ne nécessite **pas d'investissements industriels spécialisés**. En cela, elle peut faciliter la relocalisation d'activités de production dans des pays désindustrialisés comme les États-Unis ou la France, sans d'ailleurs nécessiter une main-d'œuvre abondante d'ouvriers spécialisés, devenus rares dans ces pays ;

– dans cette optique, l'impression 3D **réduit la dépendance des forces armées à leur *supply chain*** industrielle. Cet avantage est particulièrement précieux pour certaines technologies dont les conditions de fabrication n'inspirent pas la plus grande confiance. Tel est le cas, par exemple, des drones de fabrication chinoise : en imprimer des copies permet de se prémunir contre tout éventuel dispositif de suivi de leur position à distance (*tracking*) ;

– en opération, elle permet de fabriquer pièces, armes et munitions au plus près des forces, ce qui **réduit considérablement le poids de la logistique dans les OPEX**. Un tel avantage est particulièrement appréciable dans un contexte où, sur des théâtres d'opération très étendus, les convois logistiques sont à la fois vulnérables et coûteux en ressources humaines, matérielles et énergétiques. On rappellera d'ailleurs que la logistique est vue par les Russes comme l'une des faiblesses de l'OTAN ; tout moyen de la renforcer constitue donc un élément stratégique de crédibilité des forces conventionnelles du monde occidental ;

– elle simplifie la logistique en opération également en permettant de **s'affranchir des contraintes liées à l'hétérogénéité des pièces**. Le colonel

Howard Marotto a rappelé qu'en Afghanistan ou en Irak, les unités logistiques américaines avaient déplacé des « *montagnes d'acier* » de pièces détachées, mais que faute de standardisation, il en manquait toujours certaines. Or une imprimante 3D peut fabriquer nombre de pièces différentes. En cela, la fabrication additive peut réduire significativement le « *gaspillage* » de pièces en OPEX ;

– il est possible d'intégrer des capteurs dans le produit fabriqué, ce qui permet de mettre en œuvre des **systèmes d'autodiagnostic** des matériels ;

– elle permet de fabriquer des **équipements « sur-mesure »**, par exemple pour adapter la crosse d'un fusil à la morphologie d'un soldat. Plus largement, elle permet d'adapter des produits aux besoins des forces sans nécessiter de grandes compétences d'ingénierie ;

– l'impression 3D a pour effet de « ***rendre l'obsolescence obsolète*** », en ce qu'elle permet de remplacer aisément des pièces dont l'industriel n'assure plus la production dans ses usines. Dans un contexte de décalage croissant entre la durée de service des équipements militaires et les cycles industriels, ce procédé permet aux forces d'éviter des impasses (lorsque la fabrication d'une pièce n'est plus possible) ou des surcoûts (lorsque l'industriel doit recréer une chaîne de production spécialement pour les armées). Le colonel Howard Marotto a cité l'exemple d'une pièce défectueuse du char *Abrams*, que l'industriel ne pouvait fournir qu'en plus de 375 jours pour 1 500 dollars l'unité, et que la fabrication additive a permis de livrer aux forces en 33 jours (R&D comprise), pour un coût de 350 dollars ;

– une fois « industrialisé », ce procédé peut permettre, **dans certains cas, des économies**. Le colonel Howard Marotto a cité l'exemple des poignées de portes que les *Marines* sont entraînés à casser en grand nombre lors de leurs stages d'entraînement au combat en zone urbaine : l'unité coûtait 40 dollars, acheminement compris, mais avec la fabrication additive, le coût unitaire a été ramené à un dollar environ.

3. La « course » au calcul intensif

Quelles que soient les applications numériques, leur performance dépend, *in fine*, des capacités de calcul des ordinateurs qui les opèrent. D'ores et déjà, la simulation de phénomènes physiques – que ce soit pour la garantie des armes nucléaires ou pour la conception de produits industriels complexes – requiert des capacités de calcul très poussées qu'offrent les « **supercalculateurs** » – on parle de « **calcul intensif** », dit aussi « calcul à haute performance » ou *High Performance Computing* (HPC).

L'industrie informatique a longtemps été marquée par un accroissement très rapide des capacités de calcul – suivant une tendance bien connue sous le nom de « *loi de Moore* » [(1)], qui veut que la puissance de calcul d'un microprocesseur

(1) Du nom de Gordon Earle Moore, cofondateur de la société Intel.

double tous les dix-huit mois, à coût constant. Non seulement ces progrès rendent les applications existantes accessibles à un nombre de plus en plus élevé d'acteurs – États ou autres organisations –, mais surtout, elles permettent d'envisager des applications nouvelles, dont certaines intéressent les armées.

En France, outre les supercalculateurs possédés par l'industrie – y compris dans le secteur de la défense –, les supercalculateurs de recherche sont gérés :

– par le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) pour deux d'entre eux, dont l'un est consacré exclusivement aux travaux de simulation relatifs à la dissuasion nucléaire ;

– par le grand équipement national de calcul intensif (GENCI), créé en 2007 pour faciliter le partage des capacités de calcul intensif entre les organismes de recherche. L'encadré ci-après le présente.

Le grand équipement national de calcul intensif

Le grand équipement national de calcul intensif a pour vocation de **fournir des capacités de calcul intensif à la recherche et aux applications industrielles « ouvertes »** – c'est-à-dire les recherches des industriels dont les résultats sont publiés.

Il s'appuie sur **trois centres nationaux** qui hébergent les calculateurs du GENCI. L'un, notamment, est hébergé par le « très grand centre de calcul » (TGCC) du Commissariat à l'énergie atomique et aux énergies alternatives, qui est membre associé du GENCI et héberge par ailleurs plusieurs calculateurs, dont celui de l'Institut national de recherche agronomique (INRA) et celui du centre de calcul en recherche et technologie (CCRT), consacré à la recherche industrielle n'ayant pas à être publiée.

La prise de conscience de l'émergence de la « révolution numérique » en France a abouti à la création du GENCI en 2007 afin de combler un retard constaté dans le domaine du calcul intensif. Le GENCI a ainsi été institué en opérateur de recherche public, sous un statut de société civile détenue à 49 % par l'État (représenté par le ministère en charge de l'Enseignement supérieur et la Recherche), à 20 % par le CEA, à 20 % par le CNRS, à 10 % par les universités – représentées par la conférence des présidents d'université (CPU) – et à 1 % par l'INRIA. Il a pour mission de faciliter l'usage de la simulation numérique et du calcul intensif afin de soutenir la compétitivité de la France en matière scientifique et économique. Il dispose d'un budget annuel de 39 millions d'euros. Ses missions sont les suivantes :

– mettre en œuvre une stratégie nationale d'équipement en moyens de calcul intensif et de stockage de données massives au service de la recherche scientifique et industrielle française, pourvu qu'elle soit « ouverte », c'est-à-dire que ses résultats soient publiés ;

– soutenir la réalisation d'un **écosystème intégré du calcul intensif à l'échelle européenne** et y représenter la France ;

– **promouvoir la simulation numérique et le calcul intensif** auprès de la recherche académique et des industriels.

Selon les explications des dirigeants du GENCI, les projets de recherche soutenus par les capacités de calcul intensif du grand équipement **relèvent pour l'essentiel de la recherche fondamentale, de l'innovation et de l'aide à la décision publique**. Ils représentent aujourd'hui environ 600 projets par an, dont 15 % bénéficient du soutien d'un

industriel. L'attribution des heures de calcul se fait sur appels à projets annuels, les projets étant sélectionnés sur la seule base de l'excellence scientifique.

L'analyse des domaines de recherche sur lesquels portent les projets ainsi sélectionnés met en évidence les principaux domaines scientifiques pour lesquels les chercheurs français tirent le meilleur profit des moyens de calcul offerts par l'infrastructure publique : la physique, la chimie, les sciences du climat et de l'univers. Cette cartographie dessine également en creux des secteurs encore peu utilisateurs du calcul intensif, comme la biologie et la médecine, ou les sciences humaines et sociales, mais les dirigeants du GENCI ont souligné que ce sont là « *des domaines désormais en émergence dans le secteur du calcul* ». S'agissant par exemple des sciences humaines et sociales, les premières applications concernent l'urbanisme, l'archéologie, les sciences du comportement individuel et collectif, et les sciences cognitives offrent un champ de recherches prometteur – l'Institut national des sciences cognitives à Bordeaux travaille d'ailleurs en lien avec l'armée de l'air.

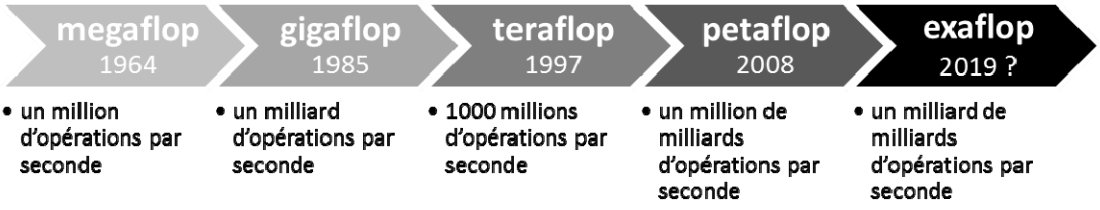
a. Un champ de rupture et de décrochage technologiques possibles

M. Philippe Lavocat, président-directeur général du GENCI, MmeMarie-Hélène Vouette, responsable de partenariats et M. Stéphane Requena, directeur de la technique et de l'innovation, ont décrit aux rapporteurs la « ***course aux capacités*** » aujourd'hui à l'œuvre en matière de calcul intensif, ainsi que les enjeux qui s'y attachent.

i. Les capacités de calcul augmentent tendanciellement

Les capacités de calcul évoluent de façon exponentielle, comme le montre le schéma ci-après. Le GENCI dispose à ce jour de calculateurs ayant une puissance dite « multi-pétaflopique », c'est-à-dire capables d'effectuer quelques millions de milliards d'opérations par seconde – soit l'équivalent de 50 000 ordinateurs portables interconnectés –, ce qui permet d'effectuer en une journée ce qu'un ordinateur de bureau mettrait 150 ans à produire. Le début de la prochaine décennie pourrait voir la mise en service de machines ayant une capacité de calcul supérieure ou égale à un exaflop par seconde, c'est-à-dire un milliard de milliards d'opérations par seconde

ÉVOLUTION DES CAPACITÉS DE CALCUL INTENSIF



Source : grand équipement national de calcul intensif (GENCI).

ii. Une compétition mondiale

La compétition internationale est très soutenue en la matière, et la Chine paraît détenir un avantage sérieux ; aux yeux de M. Philippe Lavocat, « *le calcul*

intensif, c'est un peu son programme Apollo ». Si les États-Unis ont tenu la première place de la compétition pendant plusieurs décennies, ils ont été doublés par le Japon en 2002 puis par la Chine en 2013. Celle-ci devrait disposer d'un calculateur exaflopique en 2019, avant les États-Unis en 2021, le Japon en 2022 ou l'Europe en 2022 ou 2023.

Dans cette compétition, le **niveau de financement des infrastructures** est déterminant. Selon les dirigeants du GENCI, « *au total, la France* via *le GENCI et ses trois centres investit 60 millions d'euros par an, soit la moitié de ce que dépense l'Allemagne, et d'autres puissances nous rattrapent, comme l'Italie ou la Suisse* ».

Les comparaisons internationales et européennes font ainsi apparaître un écart croissant entre le montant des investissements français et ce que les autres pays « *partenaires et / ou concurrents* » investissent dans les supercalculateurs. Les dirigeants du GENCI ont ajouté que d'ores et déjà, ces écarts ont pour résultat, en France, **une certaine difficulté à répondre aux besoins scientifiques et industriels actuels et encore plus à ceux à venir**. En effet, « *le fort taux de pression de la demande des communautés utilisatrices (représentant entre deux et trois fois les capacités disponibles) sur les calculateurs des trois grands centres nationaux ne faiblit pas, malgré les investissements passés* », tandis que l'essor du *big data* et de l'intelligence artificielle ne devrait faire qu'accroître la demande.

iii. Les usages des supercalculateurs : « *un moment historique de croisement* » entre calcul intensif, *big data* et intelligence artificielle

Selon les explications des dirigeants du GENCI, un rapprochement est aujourd'hui à l'œuvre entre :

– la simulation numérique, qui est à la fois le « *troisième pilier de la science avec la théorie (ou " modélisation") et l'expérimentation (ou "observation")* » et l'une des voies de modernisation de l'industrie ;

– le calcul intensif, dont le champ d'applications possibles croît à mesure que progressent les capacités des supercalculateurs ;

– le *big data*, c'est-à-dire l'exploitation de données dans un contexte d'« *explosion* » du volume des données disponibles, qu'elles soient instrumentales (telles que celles produites par des télescopes, des satellites, des séquenceurs génétiques, des microscopes, des réseaux de capteurs, etc.) ou « computationnelles » (comme celles générées par des simulations numériques) qu'il faut traiter et valoriser dans des délais compétitifs.

Le rapprochement entre le calcul intensif et le *big data* ouvre ainsi un nouveau champ de recherche : **l'analyse de données à haute performance** (*High Performance Data Analytics*).

iv. Une technologie utile à la maîtrise de l'intelligence artificielle

Selon les dirigeants du GENCI, l'analyse de données à haute performance « *se place en précurseur de l'intelligence artificielle* ». En effet, le **calcul intensif et l'intelligence artificielle peuvent utilement être articulés pour élargir le champ des applications possibles** de ces deux technologies :

– le calcul intensif peut apporter « *une énorme plus-value* » lors de la phase d'apprentissage des outils d'intelligence artificielle, qui repose sur d'importantes masses de données ;

– en retour, l'intelligence artificielle peut apporter au calcul intensif des outils de « post-traitement » des données produites par le calcul, en permettant d'effectuer un premier filtrage de ces données et d'accroître ainsi la productivité des chercheurs.

On en est ainsi « *à un moment historique de croisement* » entre calcul intensif, *big data* et intelligence artificielle.

b. Des applications intéressant les armées et l'industrie de défense

i. Des progrès à venir dans les applications industrielles

Avec le calcul à haute performance, l'utilisation de supercalculateurs pour des applications scientifiques ou industrielles de pointe permet des **simulations numériques de plus en plus précises pour des phénomènes de plus en plus complexes**. Dans un contexte de compétition scientifique et industrielle internationale, le recours à la simulation permet des gains de compétitivité, utiles tant à la science qu'à l'industrie : la maîtrise des techniques de modélisation et de simulation numérique devient un élément déterminant dans la R&D. D'après les dirigeants du GENCI, la simulation numérique est utilisée dans un nombre croissant de secteurs industriels, afin de réduire les temps de conception et de validation d'un produit et de faciliter ainsi l'innovation.

De plus, les applications que permet d'envisager le rapprochement entre calcul intensif, *big data* et intelligence artificielle sont nombreuses, « *pourvu que ce rapprochement soit organisé* ». Aux yeux des dirigeants du GENCI, la France dispose à cet égard de sérieux atouts, avec les champs d'excellence de la recherche et de l'industrie française, qui offrent des gisements d'applications nouvelles.

ii. Des applications possibles pour les armées

Le domaine le plus connu d'application du calcul intensif à des fins de simulation numérique dans le domaine de la défense relève de la dissuasion, et est à ce titre confié à la direction des affaires militaires (DAM) du CEA, qui opère un supercalculateur spécifique. Par nature, l'utilisation de ce calculateur pour d'autres usages et par d'autres organismes que la DAM est inenvisageable, car

incompatible avec le haut niveau de protection du secret de la défense nationale qui s'attache à la dissuasion nucléaire.

Mais pour d'autres activités militaires que la dissuasion, les dirigeants du GENCI ont fait valoir que la recherche civile (académique ou appliquée) peut être indirectement à l'origine de services et dispositifs duaux utiles à la défense nationale, citant les domaines suivants :

– **la modélisation et la simulation numérique**, qui peuvent permettre de réduire les coûts et les délais d'expérimentation dans la planification, ainsi que de connaître plus finement la configuration d'un théâtre d'opération (comme les conditions géographiques, météorologiques ou sismiques d'un terrain, ou les propriétés de matériaux) pour la planification d'actions « cinétiques » ;

– le développement de **briques matérielles et logicielles** utiles pour la défense comme pour d'autres secteurs, tels les « outils systèmes » [(1)], les « solveurs numériques » [(2)] ou les « bibliothèques d'entrées-sorties » [(3)] ;

– **la robotique** et **les drones** ;

– **l'aide à la décision**, qui se développe aujourd'hui en matière de risques industriels, de dispersion de polluants et d'agents infectieux (pour le cas d'épidémie), de séismes ou de tsunamis et autres événements climatiques extrêmes. Ces modèles d'aide à la décision peuvent aisément trouver des applications directes ou indirectes dans la planification et la conduite des opérations militaires. Tel est le cas par exemple pour les outils de gestion des répliques de séismes – qui permettent d'anticiper les dangers liés aux événements sismiques, naturels ou provoqués – et pour les outils de prévision de la diffusion de toxines – qui peuvent servir à optimiser la gestion des crises d'ordre nucléaire, radiologique, biologique ou chimique (NRBC), naturelles ou non ;

– **l'intelligence artificielle** et la « **fouille de données** » (*data mining*), notamment en lien avec des recherches en sciences humaines et sociales sur les comportements humains. Ces champs de recherches ont des applications prometteuses en matière de sécurité, de compréhension et de prévention de certains comportements, d'étude comportementale individuelle et collective, comme de repérage de signaux faibles permettant d'anticiper des menaces ou des situations à risques.

(1) Logiciels divers d'exploitation d'un matériel informatique.
(2) Outils analytiques de résolution numérique d'équations différentielles.
(3) Outils informatiques communs à nombre de systèmes et réglant divers échanges d'informations entre le processeur et les périphériques qui lui sont associés.

4. L'intelligence artificielle

En France comme à l'étranger, nombre de rapports ont été publiés sur l'intelligence artificielle [(1)]. Les rapporteurs ne s'engageront donc pas ici dans une analyse détaillée de cette technologie, pour concentrer leurs propos sur les applications qu'il est envisageable d'en faire dans les armées.

Comme le reconnaît d'emblée notre collègue Cédric Villani dans le rapport sur l'intelligence artificielle qu'il a remis en mars 2018 au Premier ministre, « *définir l'intelligence artificielle n'est pas chose facile* » ; l'encadré ci-après reprend ses éléments de définition.

Définition de l'intelligence artificielle

Depuis ses origines comme domaine de recherche spécifique, au milieu du XX^{e} siècle, l'intelligence artificielle a toujours constitué une frontière, incessamment repoussée. Elle désigne en effet moins un champ de recherches bien défini qu'un programme, fondé autour d'un objectif ambitieux : comprendre comment fonctionne la cognition humaine et la reproduire ; créer des processus cognitifs comparables à ceux de l'être humain.

Le champ est donc naturellement extrêmement vaste, tant en ce qui concerne les procédures techniques utilisées que les disciplines convoquées : mathématiques, informatiques, sciences cognitives… Les méthodes d'intelligence artificielle sont très nombreuses et diverses (ontologique, apprentissage par renforcement, apprentissage adversarial, réseaux de neurones…) et ne sont pas nouvelles : beaucoup d'algorithmes utilisés aujourd'hui ont été développés il y a plusieurs dizaines d'années.

Source : Cédric Villani, mathématicien et député de l'Essonne, « Donner du sens à l'intelligence artificielle – Pour une stratégie nationale et européenne », rapport au Premier ministre, mars 2018.

a. Un champ de R&D en plein essor

Le rapport de notre collègue Cédric Villani montre que les recherches en matière d'intelligence artificielle ont commencé il y a plusieurs décennies mais qu'elles sont entrées, « *depuis quelques années, dans une* ***nouvelle ère****, qui donne lieu à de nombreux espoirs* », principalement du fait de **l'essor de l'apprentissage automatique** (*Machine Learning*). Les technologies dites d'apprentissage profond (*Deep Learning*) – que l'on peut définir comme les méthodes plus avancées

(1) On citera notamment :
– un rapport de l'INRIA intitulé « Artificial Intelligence – Current Challenges and INRIA'S engagement *» (2016), introduction à l'intelligence artificielle et à ses applications, qui traite plusieurs enjeux : la façon de maintenir l'humain « dans la boucle » («* human in the loop *»), l'apprentissage non-supervisé, la validation et la certification des données, ainsi que l'analyse des vidéos ;*
– un rapport de la Maison-Blanche intitulé « Preparing for the future of Artificial Intelligence Artificial Intelligence *» (octobre 2016), axé sur les implications possibles de l'intelligence artificielle pour l'économie et la société américaines ;*
– le rapport de synthèse « France IA » (mars 2017), qui présente panorama de la recherche scientifique et une prospective thématique des applications de l'intelligence artificielle ;
– un excellent rapport fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (mars 2017) par nos collègues Claude de Ganay et Dominique Gillot ;
– surtout, le rapport de mission remis au Gouvernement par notre collègue Cédric Villani en mars 2018, intitulé « Donner un sens à l'intelligence artificielle – pour une stratégie nationale et européenne ».

d'apprentissage automatique, dont l'apprentissage profond constitue une sous-catégorie – connaissent en effet de brusques progrès au tournant des années 2010.

Notre collègue souligne que depuis lors, en matière d'intelligence artificielle, « *les applications se multiplient : traduction, voiture autonome, détection de cancer, etc.* », ces applications étant « *rendues possibles par des algorithmes nouveaux, par la multiplication des jeux de données et le décuplement des puissances de calcul* ».

La R&D en la matière est majoritairement le fait des entreprises privées, principalement américaines et chinoises. Comme le note un récent rapport [(1)] de nos collègues Claude de Ganay et Dominique Gillot, la concentration des technologies dans les mains de quelques sociétés crée les conditions d'une évolution vers une économie globalisée dominée par des « plateformes » numériques – notamment les « GAFA » [(2)] et les « BATX » [(3)]. Dans ce nouveau contexte économique, « *le poids pris par les grandes entreprises privées plateformistes [...] fait courir d'importants risques au principe traditionnel de souveraineté* », parmi lesquels « *un risque de redéfinition, sous l'effet de ce nouveau contexte économique, des rapports de force politiques à l'échelle mondiale* ». Le risque est bien celui, selon une expression courante, d'une « **colonisation numérique** » de notre pays par les Américains, voire les Chinois, si l'intelligence artificielle n'est pas maîtrisée par la France.

b. Un domaine dans lequel la DGA a peu investi jusqu'à présent

La directrice de la stratégie de la DGA a reconnu que le ministère n'a peut-être pas assez soutenu le travail de recherche amont en matière d'intelligence artificielle, au motif que ces technologies étaient financées par le secteur civil. Or les technologies civiles ne s'avèrent pas transposables aux équipements militaires aussi facilement que prévu. En effet, les systèmes militaires sont trop différents des civils – ne serait-ce qu'en matière de cybersécurité ou de fonctionnement hors réseau – pour que la R&D civile assure seule les études de levée de risques nécessaires à l'emploi d'une technologie dans les armées.

La DGA doit donc « remonter en puissance » en la matière, pour consacrer davantage de ses ingénieurs à ce champ de recherches. Selon Mme Caroline Laurent, la DGA en compte aujourd'hui une dizaine, et l'idéal serait à ses yeux qu'ils soient environ 200 vers 2022.

Pendant l'examen en première lecture à l'Assemblée nationale du projet de loi de programmation militaire pour les années 2019 à 2025, la ministre des Armées a annoncé le lancement d'un plan de soutien à la R&D en matière d'intelligence artificielle, précisant que les Armées investiraient « ***100 millions***

---

(1) Rapport n° 4594 (14e législature) fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques par nos collègues Claude de Ganay et Dominique Gillot, mars 2017.

(2) Google, Apple, Facebook *et* Amazon.

(3) Baidu, Alibaba, Tencent *et* Xiaomi.

d'euros par an dans l'intelligence artificielle ». Les rapporteurs ne peuvent que se féliciter de cet effort accru d'investissement.

Un tel investissement est explicitement recommandé par le rapport précité de notre collègue Cédric Villani, qui voit même dans le secteur de la défense et de la sécurité l'un des quatre domaines dans lesquels la recherche et l'industrie françaises peuvent conquérir une place de premier rang mondial. L'encadré ci-après présente le raisonnement qui conduit à identifier ainsi le secteur de la défense comme particulièrement prometteur.

Le secteur de la défense, un domaine particulièrement prometteur pour les développements de l'intelligence artificielle

Pour renforcer l'écosystème français et européen de l'intelligence artificielle, il nous faut tirer parti des avantages comparatifs et des niches d'excellence de notre économie. En d'autres termes, il nous faut déterminer les secteurs prioritaires dans lesquels notre industrie peut sérieusement envisager jouer un rôle de premier plan au niveau mondial et concurrencer les géants extra-européens. Les contraintes budgétaires nous imposent par ailleurs de refuser des logiques de saupoudrage : le soutien public à l'innovation doit se concentrer sur les secteurs où les opportunités sont les plus importantes à court et moyen termes.

Ces choix portent sur des secteurs qui ont acquis une **maturité suffisante** pour lancer des **opérations de transformation majeures** qui nécessitent des investissements importants.

Comment identifier ces secteurs stratégiques ? Notre collègue Cédric Villani s'appuie sur sept critères ainsi présentés :

– Impact : celui-ci doit être **porteur de profondes transformations** d'un point de vue économique, mais également **en termes d'intérêt général** ;

– Écosystème : la capacité à amorcer et entretenir une dynamique impose de disposer au préalable d'un **socle d'acteurs publics et privés solides** sur lequel s'appuyer ;

– « **Carburant initial** », ce que le rapport de notre collègue définit comme des ressources disponibles en matière de données, de cas d'usage, de connaissances « métier », de cadre réglementaire souple, ou de marchés envisageables. Il souligne que les données en sont un élément essentiel et constituent un avantage comparatif important ;

– **Finances et ressources humaines** : l'élément financier reste bien sûr crucial tout en étant insuffisant, les secteurs identifiés doivent être en mesure de mobiliser à la fois des financements publics et des financements privés, ainsi que les ressources humaines nécessaires ;

– **Marchés et ouverture** : la capacité pour les acteurs à faire valoir leur savoir-faire sur des marchés publics, privés, en France et à l'international est également importante dans une perspective de passage à l'échelle et afin de voir émerger des écosystèmes de grande envergure ;

– **Dualité et percolation des domaines** : quand bien même l'effort est particulièrement mis sur certains domaines, ceux-ci sont également choisis pour permettre un effet de percolation des technologies (c'est-à-dire qu'une technologie développée dans un domaine sera rapidement transposable à un autre) ;

– **Impulsion de l'État** : enfin, il faut que les secteurs nécessitent une **intervention initiale forte de l'État pour se transformer, ce qui n'est pas valable pour une grande majorité de secteurs industriels**.

En considérant ces exigences, la mission conduite par notre collègue Cédric Villani retient comme particulièrement prometteurs quatre secteurs en particulier : la santé, les transports et les mobilités, l'environnement et le secteur de la défense et de la sécurité.

Source : op. cit.

c. De vastes champs d'applications possibles, qui pourraient conférer aux forces l'ascendant opérationnel

L'intelligence artificielle ayant vocation à irriguer l'ensemble des développements informatiques, il est par nature difficile d'en prévoir tous les usages, ou d'en délimiter un champ. Il est néanmoins certain que les technologies d'intelligence artificielle trouveront des applications tant dans les systèmes opérationnels que dans les systèmes d'administration et de gestion.

i. Des applications « tous azimuts », encore insoupçonnées pour certaines

Comme le souligne notre collègue Cédric Villani, l'intelligence artificielle permettra des gains d'efficience importants dans le domaine de l'optimisation, quel que soit son champ d'application. Il cite notamment les retombées économiques que pourrait avoir l'intelligence artificielle appliquée à l'optimisation sur « *toute la logistique* », sur la planification ou la résolution de contraintes.

Pour lui, « *plus généralement, l'ensemble des domaines faisant appel à de la modélisation jusqu'ici obtenue par l'application des premiers principes, se retrouvent confrontés à des modèles alternatifs que l'on peut construire à partir des données – la voie idéale consistant sans doute à faire coopérer les deux approches pour obtenir le meilleur des deux mondes* ». Les recherches entreprises d'ores et déjà sur les applications de l'intelligence artificielle permettent ainsi d'espérer d'importants gains d'efficience dans le domaine « organique » autant qu'en matière opérationnelle.

ii. Des applications opérationnelles que l'on commence à entrevoir

Comme l'a dit M. Gérard de Boisboissel, secrétaire général de la chaire de cyberdéfense et de cybersécurité de Saint-Cyr, l'intelligence artificielle peut offrir « *une meilleure réactivité aux machines autonomes* » et une aide à la décision au commandement. Cela suppose que soit acquise une certaine confiance dans ces applications, que les usages évoluent en matière de commandement, mais aussi que soient développés des mécanismes de résilience pour le cas où les applications concernées devraient ne plus être disponibles.

C'est notamment en matière de commandement et de conduite des opérations que l'intelligence artificielle paraît permettre des gains d'efficacité opérationnelle de la façon la plus rapide et la plus décisive. Les représentants

d'IBM rencontrés à Washington ont d'ailleurs présenté aux rapporteurs les premiers résultats de leurs travaux sur les apports possibles de l'intelligence artificielle pour les fonctions de *Command and Control* (C2). Pour eux, « ***on en vient à une guerre d'algorithmes*** » et, dans ce cadre, les chaînes de commandement doivent s'adapter.

À leurs yeux, de façon générale, les systèmes automatisés permettront de trier les informations et de **présenter aux humains, à tous les échelons de commandement en même temps, les seules informations utiles**. Aujourd'hui, la chaîne de commandement et de conduite des opérations est « *relativement lente, ne serait-ce que pour que chaque échelon se fasse son idée sur la situation tactique* ». Entre la captation des données, leur transfert, leur traitement, leur analyse et l'exploitation de l'information qui en ressort, **les délais se mesurent aujourd'hui « *en heures* »**, alors que l'impératif d'efficacité opérationnelle, notamment dans la lutte contre le terrorisme, exige un traitement des données en temps réel. Le recours à l'intelligence artificielle pour l'analyse et le tri des données permet ainsi de « *passer de quelques heures, au mieux de quelques dizaines de minutes, à quelques secondes* ».

Les responsables d'IBM ont surtout fait valoir qu'avec la multiplication des capteurs, le *Department of Defense* et d'autres agences ou départements ministériels recueillent des masses de données trop considérables pour être traitées par les moyens classiques, essentiellement humains, d'**appréciation des situations**. Ce « *déluge de données* » concerne particulièrement les images, notamment avec le développement de la vidéosurveillance. C'est pourquoi le Pentagone investit dans des technologies de ***Visual Analytics*** (1), comportant par exemple des algorithmes d'analyse d'image ou de reconnaissance faciale approfondie, c'est-à-dire déjouant certains déguisements.

Aussi, selon IBM, le principal défi technologique en la matière consiste-t-il à « ***placer l'intelligence directement sur le capteur*** », ce qui doit permettre de ne transmettre aux centres de commandement que des informations « utiles », sans engorger ni les canaux de transmissions ni les capacités d'analyse et d'exploitation du renseignement. « *C'est un* ***chantier majeur pour le gouvernement américain*** ». En effet, pour IBM, les militaires ne veulent ni ne peuvent perdre de temps en analyse poussée de toutes les données que collectent leurs capteurs : « *ce qui les intéresse, c'est l'information, pas le travail des données* ». Les critères suivant lesquels c'est l'intelligence artificielle qui trie les données à fournir aux différents échelons de C2 constituent donc une question clé ; ils doivent en effet reposer sur un équilibre optimal entre cinq exigences précitées dites des « 5 V ».

(1) Champ technologique que Thales définit comme l'exploitation et la visualisation interactive des données à partir d'algorithmes d'analyse visant à « répondre au besoin d'exhaustivité *».*

d. Un défi pour la R&D et la BITD françaises

Par son caractère transverse et son développement rapide, l'essor de l'intelligence artificielle présente tous les aspects de ce qu'il est convenu d'appeler un « changement de paradigme » – un *game changer*. L'intelligence artificielle est en effet appelée à modifier tant le fonctionnement des systèmes de combat que des plateformes, des armes, des systèmes de soutiens et même des capacités de production des équipements militaires. Cependant, permettre aux armées d'exploiter pleinement et effectivement le potentiel de l'intelligence artificielle constitue un défi pour la R&D et la BITD françaises.

i. Un large champ de recherches et de développements

Les rapporteurs ont tenu à prendre la mesure de ces changements en étudiant les enjeux de l'intelligence artificielle tels que les perçoit, à titre d'exemple, Naval Group. M. Éric Papin, directeur de l'innovation et de la maîtrise technique, a expliqué que pour un grand industriel « systémier », l'intelligence artificielle revêt trois enjeux : un enjeu capacitaire, dans la mesure où l'intelligence artificielle peut conférer un avantage opérationnel aux bateaux ; un enjeu de simplification des usages ; un enjeu industriel d'amélioration de la productivité pour la production et la maintenance des équipements. Selon lui, l'intelligence artificielle pourrait avoir neuf domaines critiques d'application :

– cinq dans le champ opérationnel : les **systèmes de direction de combat**, les **systèmes d'aide au commandement**, les **systèmes de conduite** des navires, les systèmes d'armes intégrant des **drones et autres éléments de robotique**, et la **simulation** appliquée à la formation des militaires ;

– trois dans des fonctions dites « transverses » : le champ **cybernétique**, le **MCO** et les **interfaces homme–machine** ;

– un dans le champ industriel, que l'on pourrait résumer comme fondant « *l'usine du futur* » et le « jumeau numérique ».

Aussi Naval Group poursuit-il des projets de R&D dans quatre principaux domaines d'application de l'intelligence artificielle :

– la **perception de l'environnement** naval, avec des systèmes de classification d'images et d'interprétation de scènes, c'est-à-dire d'analyse du comportement des acteurs dans l'espace observé ;

– les **aides à la décision**, allant de systèmes de fusion d'informations de nature hétérogène consistant par exemple à agréger les données issues d'un radar et d'un sonar, à des systèmes d'optimisation de la décision tactique ;

– les **interfaces homme–machine**, avec des systèmes qui pourraient passer par la voix (c'est-à-dire des assistants vocaux), ou adapter un message au

niveau de fatigue ou de concentration de son destinataire, voire au profil psychologique ou cognitif de celui-ci ;

– **l'autonomie décisionnelle**, qui ne concerne pas seulement le concept de robots, mais aussi d'autres systèmes autonomes. L'intelligence artificielle pourrait alors conduire, par exemple, à la confirmation d'une information par un deuxième capteur en cas de doute sur l'interprétation des données d'un premier capteur ; à mettre en œuvre une architecture de prévision et de décision reposant sur des algorithmes de prise de décision dans un environnement incertain ; à produire des éléments de justification des décisions, d'autant plus nécessaires qu'il paraît probable, pour des systèmes d'armes, que des systèmes autonomes ne pourront être mis en œuvre que si l'on peut justifier *a posteriori* la pertinence du modèle d'intelligence artificielle retenu.

ii. Un préalable : amener l'intelligence artificielle à justifier ses résultats pour la rendre effectivement employable dans les armées

M. William Roper, directeur du *Strategic Capabilites Office* (SCO) du *Department of Defense*, a fait valoir que le recours à l'intelligence artificielle, dans un contexte de vulnérabilités cybernétiques croissantes, suppose « *une guerre permanente de l'information* » pour « *s'assurer que l'intelligence artificielle n'a pas été trompée ou faussée* » et, ce, non seulement pour éviter le dysfonctionnement de systèmes militaires reposant sur l'intelligence artificielle, mais avant tout pour permettre l'exploitation de systèmes d'intelligence artificielle dans les armées.

En effet, dans un État de droit, l'engagement de la force ne se fait que sous le **contrôle souverain des autorités politiques**, ce qui suppose que les autorités militaires puissent justifier les décisions qu'elles leur proposent, surtout si celles-ci ont des conséquences létales. Or **l'intelligence artificielle, aujourd'hui, n'est capable ni d'expliquer, ni de justifier ses décisions** ; M. William Roper a rappelé que le système d'intelligence artificielle qui a battu le champion du monde de jeu de go a effectué dix-sept mouvements que ses programmateurs ne pouvaient pas expliquer. **L'intelligence artificielle n'est donc pas opérationnelle** pour l'heure ; la rendre utilisable en opération constitue encore un vaste champ de R&D.

Cette difficulté est d'ailleurs relevée par notre collègue Cédric Villani, qui note que « *nous sommes incapables aujourd'hui de garantir* a priori *le comportement d'un système d'apprentissage* » et en conclut que « *le respect de cette exigence nécessite le développement procédures, outils et méthodes permettant d'auditer ces systèmes afin d'en évaluer la conformité à notre cadre juridique et éthique* ».

Il préconise donc des travaux visant à rendre les systèmes d'intelligence artificielle capables d'expliquer leurs résultats, ce qui renvoie au concept

d'« **explicabilité** » qui sous-tend certaines dispositions de la loi pour une République numérique [(1)] et du droit européen de la protection des données [(2)].

Il est ainsi **urgent de soutenir la recherche sur l'« explicabilité » de l'intelligence artificielle** suivant trois axes de travaux interdisciplinaires, faisant intervenir mathématiques, *design*, neurosciences comme psychologie :

– la production de modèles « *plus explicables* » ;

– la production d'interfaces utilisateur « *plus intelligibles* » ;

– la compréhension des mécanismes cognitifs à l'œuvre.

Compte tenu de la gravité potentielle des effets des systèmes d'armes, les travaux visant à rendre les systèmes d'intelligence artificielle capables de fournir des justifications de leurs propres résultats doivent être vus comme un préalable à l'exploitation des technologies d'intelligence artificielle. D'ailleurs, la DARPA a d'ores et déjà lancé un programme d'étude sur l'« explicabilité » de l'intelligence artificielle, que présente l'encadré ci-après.

Le programme « *Explainable AI* » de la DARPA

En août 2016, la DARPA a lancé un appel à propositions destiné à soutenir la recherche sur l'« explicabilité » de l'intelligence artificielle. Identifié comme une priorité majeure pour le secteur de la défense, ce programme vise à financer le développement de systèmes d'intelligence artificielle explicables par construction.

Si le montant global du financement disponible n'a pas été rendu public, les premières informations disponibles sur les projets retenus (treize au total) laissent soupçonner que celui-ci se chiffre en plusieurs dizaines de millions d'euros. À elle seule, l'université d'État de l'Oregon a obtenu 5,2 millions d'euros sur trois ans pour le financement de huit chercheurs en apprentissage automatique.

Source : op. cit.

5. Les systèmes autonomes, robots et drones

Comme le note le Secrétariat général de la défense et de la sécurité nationale (SGDSN) dans une étude de prospective technico-opérationnelle intitulée « Chocs futurs » [(3)], il n'y a pas de définition consensuelle des « systèmes autonomes ». Les rapporteurs retiendront donc celle du SGDSN, qui qualifie de systèmes autonomes les « *objets physiques ou " intangibles" dotés de fonctions complexes comme l'orientation, la navigation, le déclenchement ou l'arrêt d'effecteurs* ».

(1) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

(2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, communément appelé General Data Protection Regulation *(règlement général sur la protection des données).*

(3) Secrétariat général de la défense et de la sécurité nationale, « Chocs futurs – Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité », mai 2017.

a. L'essor prévisible des systèmes autonomes

i. Vers des systèmes de plus en plus autonomes

Selon une typologie établie par le document précité du SGDSN, l'autonomie des systèmes peut être :

– **nulle, auquel cas le système est télé opéré**, c'est-à-dire piloté à distance par un équipage, *via* des moyens de télécommunication. Dans ce cas, l'équipage accomplit à distance les mêmes tâches que s'il était embarqué. On peut ainsi assimiler les drones à cette catégorie de systèmes autonomes ;

– **partielle, pour les systèmes « télé supervisés »**, dont certaines tâches (comme la navigation, l'observation ou le pointage des capacités de tir) sont automatisées. *Via* des moyens de télécommunication, un opérateur analyse la situation et contrôle l'exécution des tâches les plus sensibles, comme, par exemple, le pointage des armes et l'ouverture du feu ;

– **complète, dans le cas d'un système autonome au sens strict**, c'est-à-dire qui exécute sans intervention humaine l'ensemble de ses tâches, y compris les plus sensibles, lesdites tâches lui étant cependant explicitement assignées avant le début de sa mission. L'étude « Chocs futurs » signale un type particulier de système autonome, qui « *focalise aujourd'hui l'attention* » : le système d'arme létal autonome (SALA), que l'on peut définir comme « *un système robot disposant d'une part d'autonomie plus ou moins développée et qui mène par lui-même, de par sa conception, des missions de destruction* ». Tel est le cas de certaines torpilles et de certains missiles « rôdeurs ».

D'ores et déjà, note le SGDSN, plusieurs puissances – y compris la France – disposent aujourd'hui de systèmes d'armes, « *y compris létaux, intégrant des robots* » ou des systèmes autonomes. Il peut s'agir par exemple de certains systèmes de drones armés ou plateformes disposant de fonctions automatisées, comme le pilotage ou le ciblage automatique. Les développements technologiques prévisibles en matière de robotique, nourris par les progrès à venir en matière d'intelligence artificielle, permettront de développer **des systèmes de plus en plus autonomes**.

ii. Vers des possibilités opérationnelles de plus en plus larges

Comme l'a dit M. Gérard de Boisboissel, **les développements du champ de la robotisation ouvrent ainsi un grand champ d'opportunités** pour nos forces dans la numérisation de l'espace de bataille. La robotisation participe en effet à une nouvelle évolution dans l'art de faire la guerre « *en accroissant les capacités tactiques multi-milieux et en déportant plus loin des effets* », tout en **préservant le soldat**, que le déploiement de robots en première ligne permet d'éloigner du danger et que les systèmes autonomes permettent de décharger de certaines tâches chronophages. Les systèmes robotisés permettront à nos forces de conserver une supériorité tactique sur le terrain, « *supériorité mise à mal par*

l'utilisation par nos ennemis de nouvelles technologies issues du monde civil impliquant de nouvelles menaces à prendre en compte ».

L'étude « Chocs futurs » prévoit que **robots et systèmes autonomes seront « omniprésents » sur le champ de bataille**, dans les trois milieux. En permettant d'assurer une couverture permanente dans le milieu aérien ou maritime, ils offriront un sérieux ascendant opérationnel. Dans le milieu terrestre, également, ils deviendraient indispensables dans l'environnement des forces, pour l'appui ou le soutien des forces terrestres ainsi que pour leur renseignement. Cette étude prédit aussi une miniaturisation des robots, qui se verraient intégrer des technologies d'intelligence artificielle, ce qui conduit à « *envisager leur déploiement futur sous forme d'**essaim de robots** plutôt qu'en termes de plateformes coûteuses, peu nombreuses et exposées aux coups* ». Des expérimentations américaines sont d'ailleurs en cours pour ce type d'essaims autonomes et « intelligents ».

Ce sont ces perspectives qui confèrent toute leur importance aux discussions internationales menées à l'ONU, avec la participation active de la France, sur le statut des systèmes d'armes létaux autonomes dans le cadre des travaux de suivi de la convention de Genève sur certaines armes classiques [(1)].

b. Les programmes et les voies de développement actuels en France

i. Un retard dans l'équipement des forces françaises

Le retard pris dans le développement de drones en France est bien connu ; les rapporteurs se contenteront de relever que la directrice de la stratégie de la DGA a reconnu que « *le vecteur du drone était vu comme étant un objet suffisamment peu complexe pour qu'il n'y ait pas eu d'études amont* ». Elle a néanmoins fait valoir que « *le* Reaper *n'a pas été financé par le Pentagone* ab initio *; ce sont les armées américaines qui l'ont choisi, après qu'il a été autofinancé par l'industriel* ».

Selon M. Gérard de Boisboissel, dans la révolution robotique en cours – qu'il qualifie de « ***robolution*** » –, la France dispose de sérieux atouts s'agissant des compétences scientifiques et technologiques, mais **manque d'industriels « intégrateurs » de ces technologies**, à la différence des États-Unis ou d'Israël.

ii. Des compétences dans l'industrie française

Les industriels français ont néanmoins conduit des recherches sur les drones. Les rapporteurs ont tiré profit de leur déplacement au centre de recherche de Naval Group à Ollioules pour faire un bilan des travaux conduits dans ce domaine par le groupe – travaux qui lui ont valu de se voir attribué très récemment un contrat d'armement pour un système de drone aérien de la marine. Le directeur

(1) Convention conclue à Genève le 10 octobre 1980 sous les auspices de l'organisation des Nations unies sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination.

des systèmes de drones de Naval Group a ainsi présenté les programmes de R&D en matière de drones navals suivis par cet industriel depuis 2005.

Le groupe a d'abord utilisé des appareils américains, puis s'est engagé dans le développement d'un système « *purement français* », se présentant comme un hélicoptère de 700 kg et 100 miles nautiques (soit 185 km) d'autonomie, portant trois charges utiles, et mû par un moteur à piston à carburant lourd, c'est-à-dire le même carburant que l'hélicoptère de bord. Un marché a été notifié à Naval Group et Airbus Helicopters au titre du programme de « **système de drone aérien pour la marine** » (**SDAM**).

Ce programme a ainsi pour enjeu de développer une filière française d'excellence dans les drones navals aériens, avec un fort potentiel d'export. Structurant pour la marine, il commencera par une phase de tests de 45 mois, probablement sur une FREMM, pour entrer ensuite en phase d'industrialisation. La cohabitation sur une même frégate d'un drone et d'un hélicoptère classique fait également l'objet d'études.

D'autres programmes, à l'image du programme d'études amont ESPADON qui a servi de fondement au programme de système de lutte anti-mines du futur (SLAMF), ont permis de lever encore d'autres risques technologiques. Naval Group a également proposé à la DGA, avec le roboticien français ECA [(1)], un programme d'études amont de drone multi-missions embarqué, du format d'une torpille, appelé Ausyris (*Autonomous Underwater System for Reconnaissance, Intelligence and Surveillance*). L'un des enjeux de ce projet consiste à assurer une articulation efficace entre les systèmes propres du drone – comme ceux de sa charge utile, de ses liaisons de données, et de ses instruments de navigation – et d'un « segment de bord » embarqué. Le drone est ainsi intégré comme un capteur déporté du bateau, s'intégrant pleinement au *combat management system* (CMS) de celui-ci.

6. L'informatique quantique

On appelle « informatique quantique » l'application des lois – souvent contre-intuitives pour les esprits contemporains – de la physique quantique à l'informatique. Comme l'ont expliqué les dirigeants du GENCI, l'avènement de l'informatique quantique constituera « *une rupture technologique et surtout conceptuelle* » ; l'ordinateur quantique utilisera en effet les propriétés fondamentales de la mécanique quantique, très différentes de celles régissant la physique classique. L'encadré ci-après en présente le principe.

(1) Société française de robotique, fondée en 1936 sous le nom d'« études et constructions aéronautiques » (ECA).

L'apport de la physique quantique à l'informatique

Plusieurs physiciens théoriciens ont imaginé, dans les années 1970, le concept de l'ordinateur dit « quantique ».

Les ordinateurs traditionnels, du simple ordinateur de bureau au supercalculateur, fonctionnent aujourd'hui avec des transistors et des processeurs, et une base binaire de codage de l'information, les fameux bits, dont la valeur peut être soit 0 soit 1. L'ordinateur quantique, lui, manipule des particules élémentaires, telles que les photons, pour représenter l'information. Ces particules, de taille infinitésimale – de l'ordre de 10^{-22} mètres – ont des propriétés dites « quantiques », en rupture avec l'approche classique déterministe, qui peuvent heurter l'intuition.

Parmi les propriétés de la mécanique quantique, le **phénomène de superposition**, qui « permet » à une particule d'« être » à plusieurs endroits en même temps, est sans doute le plus structurant. En appliquant cette idée à l'informatique, les pères fondateurs de l'informatique quantique ont cherché à tirer profit de la possibilité, pour une particule, d'être à plusieurs endroits à la fois, pour construire **un système qui pourrait effectuer plusieurs calculs en même temps**, et non plus simplement en parallèle, ce que font les ordinateurs actuellement.

Ce passage du monde classique au monde quantique est notamment symbolisé par l'utilisation des **qbits**, pendants quantiques des bits informatiques classiques, qui ne valent plus strictement 0 ou 1 de façon déterministe, mais une superposition de ces deux valeurs, avec des probabilités différentes. Très concrètement, cette approche permet aux systèmes de calcul quantique de voir leur **puissance de calcul augmenter de façon exponentielle** au fur et à mesure que leur nombre de qbits augmente – là où la croissance des machines classiques était « seulement » linéaire – ce qui laisse entrevoir des opportunités et développements extrêmement intéressants dans de nombreux champs d'application.

Source : Secrétariat général de la défense et de la sécurité nationale, « Chocs futurs – Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité », mai 2017.

a. Un domaine de possible rupture technologique susceptible d'avoir des applications majeures pour les armées

Pour ce qui intéresse les armées, les applications envisagées de l'informatique quantique sont de trois ordres principaux : l'utilisation des principes de la physique quantique à la cryptographie, même sans ordinateur quantique, pour protéger les transmissions ; l'augmentation exponentielle des puissances de calcul avec les ordinateurs quantiques, qui ouvrira un champ nouveau d'applications numériques, y compris dans le déchiffrement des moyens actuels de cryptographie ; la cryptographie dite « post-quantique », qui permettrait de sécuriser les transmissions contre un attaquant doté d'un ordinateur quantique de cryptanalyse.

i. La « cryptographie quantique », ou l'application des principes de la physique à la construction des moyens de cryptographie

Les principes de la physique quantique – notamment le principe de superposition – permet d'ores et déjà de concevoir et de construire des mécanismes de sécurisation des transmissions. Tel est l'objet des recherches dites de « **cryptographie quantique** ».

Comme l'explique l'étude « Chocs futurs » précitée, celle-ci introduit en particulier la possibilité de « *transmettre une information sans en protéger la confidentialité de prime abord, mais en garantissant la détection* a posteriori *de toute interception par une tierce partie* ». Les dirigeants de GENCI ont expliqué que le chiffrement quantique repose sur un état quantique particulier de la matière (appelé intrication quantique) que déséquilibre son décryptage, ce qui se manifeste immédiatement. Théorisée depuis plus de trente ans, cette approche de la cryptographie ne nécessite pas la mise en œuvre d'un ordinateur quantique. En cela, elle ne peut pas être vue comme une rupture technologique majeure, et ne présente d'intérêt significatif que « *dans certains cas d'usage spécifiques* », où compte moins la sécurité de l'information transmise que la garantie de son intégrité.

Il est à noter que la cryptologie quantique a d'ores et déjà été mise en œuvre dans le cadre de plusieurs programmes depuis les années 2000. On retiendra à titre d'exemple le programme chinois QUESS, avec lequel la Chine a lancé en 2016 le satellite *MOZI* afin de conduire des expériences sur la transmission d'informations à longue distance au moyen de systèmes de cryptographie quantique. Autre exemple, selon le GENCI, les Chinois associés aux Autrichiens ont démontré pour la première fois en septembre 2017 la possibilité d'une visioconférence cryptée *via* des technologies quantiques en passant par un satellite.

ii. L'« ordinateur quantique », outil d'une croissance exponentielle des puissances de calcul

Compte tenu des propriétés de la physique quantique, le rapport « Chocs futurs » donne une illustration très éclairante de la puissance de calcul qu'aurait un ordinateur exploitant les mécanismes quantiques : « *un ordinateur quantique de 300 qbits devrait avoir une puissance de calcul analogue à celle d'un supercalculateur construit avec tous les atomes de l'univers* ». Pour comprendre cet exemple en perspective avec les programmes de R&D actuels, il le met en regard avec l'ambition affichée par la société canadienne D-Wave de commercialiser prochainement un ordinateur quantique contenant 2 000 qbits. L'ordinateur quantique permettra ainsi de réduire drastiquement le temps nécessaire pour effectuer une tâche, avec pour conséquence directe de rendre vulnérables la plupart des chiffrements obtenus par les algorithmes actuels.

- *Un champ de recherche et développement comportant encore des incertitudes*

La faisabilité même d'un ordinateur véritablement quantique n'est pas encore démontrée de façon incontestable. Mais les rapporteurs ont pu constater que si les experts ont des avis divergents sur la question, leurs anticipations diffèrent moins sur la faisabilité, à terme, d'un « ordinateur quantique » que sur l'échéance de ce terme. De surcroît, ils observent que si ce terme était envisagé il y a quelques années comme très lointain, il tend aujourd'hui à se rapprocher dans les anticipations actuelles, au gré des progrès récents de la R&D. Pour illustrer ce phénomène, M. Antoine Petit, alors président-directeur général de l'INRIA, a expliqué qu'en 2012, recevant son prix Nobel, le professeur Serge Haroche disait ne pas croire qu'un « ordinateur » quantique soit possible, mais que d'autres chercheurs, six ans plus tard, en prévoient l'avènement dans cinq ou dix ans.

En effet, plusieurs industriels disposent déjà de prototypes de calculateurs quantiques. Une première machine à 2048 qbits, conçue par l'entreprise canadienne D-Wave et appelée D-Wave X2, est présentée comme quantique, même si selon les explications de M. Antoine Petit, la technologie employée – dite « de *quantum annealing* » ou « de recuit simulé quantique » – ne semble pas encore totalement répondre aux critères scientifiques pouvant la qualifier de « quantique » au sens propre.

S'agissant de la date de mise en service d'un calculateur quantique *stricto sensu*, les anticipations s'accélèrent ; l'opinion personnelle des responsables d'IBM rencontrés par les rapporteurs est que cette rupture technologique sera effective à **un horizon de cinq ans**. En tout état de cause, comme le disent les professeurs de l'*Eisenhower School*, « ***l'horizon s'approche*** », IBM et l'université du Maryland étant très avancés dans leurs recherches.

D'autres experts sont en revanche très prudents ; ainsi, par exemple, M. Marc Darmon, directeur général adjoint de Thales, a fait valoir que l'informatique quantique n'existe aujourd'hui qu'en laboratoire et estimé qu'il n'en est pas envisagé de mise en œuvre opérationnelle avant **dix ans** – ce qui demeure peu probable à ses yeux –, **voire trente ans**. Pour les dirigeants de l'INRIA, à un horizon de cinq ou dix ans, un tel « ordinateur » serait en réalité un processeur quantique ayant un nombre très limité d'applications – rien de tel qu'un ordinateur universel. C'est ce qui fait dire au SGDSN, dans l'étude « Chocs futurs » précitée, que « *rien ne permet d'affirmer que le développement d'ordinateurs quantiques sera techniquement possible d'ici 2030* ».

Quel que soit le point de vue que l'on retienne, les anticipations concernant l'éventuelle mise en service d'un ordinateur quantique s'inscrivent aujourd'hui dans un champ temporel suffisamment rapproché pour mériter d'être pleinement pris en compte dans les exercices de prospective des armées. Il est d'ailleurs cohérent avec l'horizon retenu par la programmation militaire française, qui pose des jalons pour l'équipement des forces dans les années 2040. À ce titre,

les armées ne sauraient se désintéresser des applications possibles de l'informatique quantique. Deux ordres d'applications ressortent à ce jour des travaux des rapporteurs : la cryptanalyse – c'est-à-dire la démarche consistant à « casser » un message chiffré sans connaître sa clé – et l'ensemble des opérations nécessitant une puissance de calcul massive.

- *Une rupture technologique qui sera immédiatement applicable en matière de cryptologie*

L'application la plus souvent évoquée d'un futur ordinateur quantique consiste à décrypter les dispositifs actuels de chiffrement des transmissions. Or les besoins de sécurité des transmissions d'informations vont croissant avec la numérisation des organisations, au premier rang desquelles se trouvent les armées. Là réside d'ailleurs l'intérêt des technologies dites de *blockchain*.

Or, comme l'a expliqué M. Antoine Petit, l'avantage de l'informatique quantique est qu'elle permettrait par exemple de « casser » tous les codes de cryptographie basés sur la technologie appelée « RSA » [(1)], qui consiste à multiplier entre eux des nombres premiers à beaucoup de chiffres. Selon les explications des dirigeants du GENCI, parmi les capacités de calcul qu'offre l'informatique quantique figure en effet en effet la factorisation quasi instantanée en nombres premiers. Tester toutes les combinaisons possibles prendrait aujourd'hui un temps dépassant l'entendement – l'étude « Chocs futurs » évoque « *des milliards d'années de calcul* » pour « casser » les problèmes mathématiques « *difficiles* » sur lesquels repose aujourd'hui la cryptographie de pointe. Mais un processeur quantique pourrait aisément casser ces codes.

Surtout, comme l'a fait valoir M. Guillaume Poupard, directeur général de l'ANSSI, l'ordinateur quantique, « *qui finira par exister* », prendra d'abord la forme de calculateurs de grand volume capables de résoudre des problèmes insolubles aujourd'hui et notamment de « casser » les moyens de cryptographie asymétrique, moins par une question de puissance de calcul que par la manière de calculer : plutôt que de tester plusieurs options successivement, ils les testeront simultanément.

Là encore, les prévisions de rupture technologique sont à prendre avec prudence. Selon M. Antoine Petit, les recherches en cours ont donné quelques résultats, qui ont aussi montré leurs limites : certains codes ne sont pas réellement maniables. De même, M. Brian Pierce, directeur du service de l'innovation informatique (*Information Innovation Office*) de la DARPA, a estimé que certaines technologiques quantiques, comme celles de la société D-Wave, ne sont pas applicables aujourd'hui à la cryptographie.

(1) Des initiales des trois mathématiciens inventeurs de cette technologie en 1977 : Ron Rivest, Adi Shamir et Len Adleman.

- *Une rupture technologique qui pourrait ouvrir la voie à une intensification sans précédent du combat cybernétique*

Les responsables d'IBM rencontrés par les rapporteurs ont fait valoir qu'au-delà des applications de cryptanalyse, l'ordinateur quantique représentera une rupture technologique dans de nombreux champs d'applications, qui appellera à un changement radical de tous les équipements informatiques en raison du caractère quasiment infini que prendront les capacités de calcul.

En effet, les algorithmes actuels sont contraints par la puissance de calcul des machines ; les algorithmes quantiques ne le seront pas. Par exemple, en matière de *Command and Control*, si les algorithmes non-quantiques permettent de réduire les délais de traitement des informations de quelques heures à quelques secondes, le quantique ramènera ce délai en deçà de la seconde. De façon générale, **l'informatique quantique constituera la base de toutes les technologies d'intelligence artificielle ou de *big data*** ; « *la course au quantique est donc une course cruciale* ».

iii. La cryptologie « post-quantique » et la sécurisation des transmissions face aux ordinateurs quantiques

Pour incertaine qu'elle soit, l'application de l'informatique quantique à la cryptanalyse constitue donc bien un risque qu'il serait imprudent de ne pas prendre en compte, tant pour les possibilités de décryptage des transmissions adverses qu'elle offre que pour les vulnérabilités qu'elle créerait pour nos propres forces si un adversaire s'en trouvait doté.

Il faut donc s'y préparer avant qu'advienne cette grave menace pour nos systèmes de cryptographie ; tel est l'objet des programmes de simulation de l'informatique quantique, qui visent à préparer des codes non « cassables » par un ordinateur quantique. Ce champ de recherche est appelé « **cryptologie post-quantique** ».

La théorie n'a pas encore tranché la question de savoir si la cryptologie post-quantique devra nécessairement s'appuyer sur des ordinateurs quantiques ou si elle demeure possible avec des moyens classiques. Certains observateurs n'envisagent de cryptologie post-quantique que mise en œuvre par des moyens quantiques ; d'autres ont une position différente.

Ainsi, M. Brian Teeple, adjoint de la *Chief Information Officer* du Pentagone en charge des fonctions dites de « C4&IIC » – pour *Command, Control, Communications & Computers* (C4) et *Information Infrastructure Capabilities* (IIC) – a indiqué que l'analyse des services Pentagone diverge de celle des industriels et de certains scientifiques concernant la cryptographie. Pour le *Department of Defense*, **une protection non-quantique demeurera possible même face aux attaques d'un ordinateur quantique**. Un certain nombre d'ajustements techniques devraient ainsi permettre de rendre les systèmes de

cryptographie non-quantiques actuels à même de résister à la puissance du calcul quantique, car « *le quantique résoudra certains problèmes mieux que l'informatique actuelle, mais pas tous* ». De même, M. Marc Darmon, directeur général adjoint de Thales a reconnu qu'à court terme, un ordinateur quantique pourrait casser les algorithmes asymétriques actuellement employés dans tous les systèmes de cryptologie, mais qu'il est envisageable de définir de nouveaux algorithmes asymétriques résistants aux moyens quantiques de cryptanalyse et de doubler les tailles des clés des algorithmes symétriques. Selon lui, une fois trouvés de tels algorithmes, la recherche en cryptologie ne devrait d'ailleurs pas être beaucoup plus coûteuse qu'aujourd'hui.

Un ensemble de recherches visant à définir ces nouveaux standards est conduit aujourd'hui et doit aboutir dans trois à cinq ans ; aux États-Unis, l'Institut national des standards et de la technologie – *National Institute for Standards and Technology* (NIST) – a d'ailleurs lancé un concours destiné à la communauté mondiale du chiffrement, l'appelant à proposer des algorithmes susceptibles de résister aux machines quantiques. En France, Thales et la direction de la maîtrise de l'information de la DGA étudient les principaux domaines sur lesquels sont basées ces propositions. Globalement, la recherche française est d'ailleurs bien placée, un nombre non négligeable des propositions soumises à la compétition ouverte par le NIST sont, selon Thales, « *fortement françaises* ».

b. Un secteur dans lequel la recherche est intense et les atouts français précieux à conserver

i. Une compétition internationale revêtant de considérables enjeux souverains, technologiques et économiques

Conserver un niveau satisfaisant de sécurité des transmissions cryptées, voire élargir nos possibilités de décryptage des communications adverses chiffrées, revêt un évident enjeu de souveraineté pour une puissance militaire de haute technologie comme la France. On relèvera à cet égard que la première machine *D-Wave X2* à 2048 qbits présentée comme quantique, acquise en 2013 par *Google*, est hébergée par le laboratoire Ames Research Center de la NASA et que l'entreprise *D-Wave* est financée notamment par *Amazon* – ainsi que, dit-on, par certains services américains.

De surcroît, la maîtrise de l'informatique quantique revêt aussi un intérêt technologique plus large. En effet, cette technologie apparaît aujourd'hui comme prometteuse d'un nouvel élan de progrès dans l'informatique, au moment où la croissance continue des performances des outils classiques en matière de calcul risque de connaître une asymptote du double fait de la consommation électrique considérable des équipements et du seuil « plancher » que représente l'atome pour la taille des gravures des composants informatiques. Un nouveau bond dans le progrès de la puissance de calcul disponible ouvrirait alors des possibilités nouvelles dans tous les champs d'application du calcul intensif décrits *supra*, notamment la simulation et l'optimisation.

En conséquence, les retombées économiques de l'informatique quantique pourraient être importantes. D'ailleurs, ce domaine technologique constitue un champ de recherches intensives aux États-Unis. À titre d'exemple, l'informatique quantique constitue avec le *cloud* les deux principaux domaines des budgets d'investissement d'IBM – soit cinq milliards de dollars par an. Selon IBM, les technologies informatiques « classiques » ne sont plus vues par les industriels comme un axe de développement majeur, même s'agissant de puces neuro-morphiques, c'est-à-dire reproduisant un système neuronal.

ii. Un champ dans lequel les atouts français méritent d'être préservés et exploités

La R&D européenne est loin d'être « hors–jeu », et les Français s'y placent aujourd'hui au premier rang. Atos Bull a ainsi mis en œuvre une machine capable de simuler jusqu'à 40 bits quantiques, appelée « Atos *Quantum Learning Machine* » (Atos QLM). M. Thierry Breton, président-directeur général d'Atos, a déclaré : « *en dévoilant aujourd'hui le simulateur quantique commercial le plus performant au monde, Atos confirme à la fois son ambition d'industriel* leader *en Europe et la vocation qui est la sienne d'accompagner ses clients dès le début de ce qui s'annonce être la future évolution technologique majeure des années à venir. La physique quantique va engendrer de profondes mutations notamment dans le domaine de la cybersécurité, l'une des priorités stratégiques des organisations. Nous nous devons d'en anticiper dès aujourd'hui les conséquences. Les équipes du laboratoire d'Atos Quantum ont fourni des efforts remarquables, reconnus et soutenus par un Conseil scientifique de renommée internationale, pour fournir dès à présent aux chercheurs et ingénieurs du monde entier un environnement de simulation leur permettant de développer des algorithmes quantiques et se préparer aux accélérations majeures à venir* ».

La compétition se joue aussi sur le terrain de la préparation de l'ensemble de l'environnement informatique à l'arrivée d'un ordinateur quantique. En effet, comme l'ont expliqué les dirigeants du GENCI, l'informatique quantique « *changera les modes de pensée de façon radicale* ». La technologie ne pourra être maîtrisée, vers 2025-2030, qu'**après des exercices de simulation préparatoires à la découverte et à l'usage des diverses possibilités**, qui constitue le véritable enjeu des travaux actuels. Les recherches en cryptologie post-quantique en participent ; d'ores et déjà, Atos travaille d'ailleurs à concevoir des algorithmes de sécurisation dits « *quantum safe* » – résistants aux moyens quantiques.

Compte tenu de la longue tradition d'excellence scientifique française en matière de mathématiques, **la concurrence internationale est pour l'essentiel une question de moyens**. Aux yeux de Thales, l'avance des Français sur les autres Européens est nette, tant en matière technique avec les équipes de la DGA et de Thales, qu'en matière de doctrine avec l'ANSSI. Elle mérite d'être confortée pour ne pas se trouver dépassée par ses concurrents.

7. Les convergences entre neurosciences et numérique

Si les idées d'« homme augmenté » ou de contrôle du système cognitif humain par des machines sont restées pendant de longues décennies l'apanage de la science-fiction, les développements récents de la science leur confèrent aujourd'hui la valeur d'un champ de recherche scientifique crédible. Des convergences sont en effet à l'œuvre entre les neurosciences, les nanotechnologies, les biotechnologies, les sciences de l'ingénieur et l'informatique, qui favorisent le développement de nouveaux outils et de nouvelles méthodes d'intervention au niveau cérébral.

Les applications militaires des résultats envisageables de ces recherches, bien que lointaines dans le temps et difficiles à cerner avec précision dans leurs modalités, ne peuvent pas être ignorées. Pas plus, d'ailleurs, que ne le sont les questions éthiques majeures qu'elles soulèvent, et qui méritent d'être traitées en amont des découvertes scientifiques et d'éventuels investissements.

a. Les programmes de recherche en neurosciences aboutissent à des résultats que ne peut ignorer la défense

- *Un champ d'investissement*

Depuis les années 2000, les neurosciences font l'objet d'investissements importants au travers de plusieurs grands programmes emblématiques, tels que :

– le programme *Human Brain Project* lancé en 2013 par la Commission européenne et doté de 1,2 milliard d'euros, qui vise à réaliser une simulation numérique complète du cerveau humain grâce à un supercalculateur ;

– l'initiative américaine BRAIN (*Brain Research through Advancing Innovative Neurotechnologies*), lancé la même année et doté de 4,5 milliards de dollars, qui vise lui aussi à mieux comprendre le fonctionnement du cerveau humain, à développer de nouvelles technologies et à soutenir la R&D en matière de neuro-technologies ;

– un récent programme chinois visant à comprendre les circuits neuronaux à l'origine des fonctions cognitives et les mécanismes à l'œuvre dans les maladies cérébrales.

- *Des avancées significatives dans un champ d'application dual*

Les recherches récentes s'orientent suivant deux axes majeurs :

– l'exploration cérébrale, facilitée depuis les années 1990 par l'imagerie à résonance magnétique fonctionnelle, qui connaît des avancées majeures avec les développements de l'optogénétique, laquelle permet aujourd'hui d'observer et de contrôler l'activité de groupes de neurones par des *stimuli* lumineux ;

– les développements d'interfaces cerveau–machines, c'est-à-dire d'outils qui permettent au cerveau de contrôler des appareils extérieurs ou, inversement, à des instruments extérieurs d'avoir une action directe sur les neurones. L'encadré ci-après présente certains résultats de recherches en la matière.

Les avancées récentes en matière d'interfaces cerveau-machines

● Le centre de recherche *Clinatec* de Grenoble travaille sur un exosquelette qui pourrait être contrôlé par une interface transmettant les ordres du cerveau, pour des patients paraplégiques.

● Un essai de quelques minutes réalisé par la société *TEKEVER* en 2015 dans le cadre du programme européen *Brainflight*, qui vise à développer des outils de commande cérébrale pour le secteur aérien, a montré qu'il était possible de piloter un drone par la pensée, le pilote étant muni d'un casque à électrodes détectant l'activité cérébrale. La même année, une patiente paraplégique atteinte d'une maladie neurodégénérative, après avoir pu commander un bras grâce à des microélectrodes implantées dans son cerveau, a réussi, après reprogrammation du dispositif, à piloter un avion de chasse F35 en simulateur.

● Une équipe conjointe au *Karlsruhe Institute of Technology* en Allemagne et au *Wadsworth Center* aux États-Unis a réussi à restituer des phrases entières pensées en langage naturel, par l'enregistrement des ondes cérébrales *via* des électrodes intracrâniennes.

● Des chercheurs de la *Duke University* ont publié en 2015 les résultats de deux séries de recherche portant sur la construction d'un dispositif informatique organique à l'aide de plusieurs cerveaux interconnectés, dispositif qu'ils ont baptisé *brainet* (contraction de *brain* et de *network*). Ils ont pu montrer que des singes ou des rats étaient capables de coordonner des signaux cérébraux afin de réaliser une action commune – par exemple, déplacer un bras virtuel pour atteindre une cible, afin d'obtenir une récompense.

Source : op. cit.

Les perspectives d'application de ces recherches sont nombreuses. Elles vont de la restauration de fonctions humaines altérées – comme l'ouïe, la vue ou la motricité – à l'amélioration de ces fonctions. Donc, schématiquement, de l'« homme réparé » à l'« homme augmenté ».

En outre, ces recherches sont aussi de nature à contribuer au développement de l'intelligence artificielle. À cet égard, les responsables d'IBM ont souligné l'intérêt du projet européen de modélisation informatique du cerveau humain, dans la mesure où il pourra contribuer notamment à **améliorer les technologies d'apprentissage par la machine**, dites de *Machine Learning*, qui constituent la première étape de la programmation d'une intelligence artificielle. Ces technologies sont en effet aujourd'hui biaisées, car elles restent supervisées par des humains. « *Aucune intelligence artificielle n'apprend par elle-même, ou en discutant entre systèmes d'intelligence artificielle* » ; or la supervision de l'apprentissage par un humain crée nécessairement des biais cognitifs, comme tout parent en crée dans l'éducation de ses enfants. Le *Machine Learning* gagnera donc à ne plus reposer sur un cerveau humain pour « apprendre à apprendre » à une machine.

b. Sous réserves d'épineuses questions éthiques restant à trancher, les applications militaires des neurosciences sont nombreuses

Signe de l'intérêt que le secteur de la défense peut trouver dans le développement des technologies découlant des neurosciences, on soulignera que *via* la DARPA, le *Département of Defense* américain finance plusieurs programmes de R&D dans le cadre de l'initiative américaine BRAIN. L'encadré ci-après présente la teneur de ces recherches.

Les programmes de recherche du Pentagone dans le champ des neurosciences

La DARPA a initié un certain nombre de programmes avec des objectifs variés, comme favoriser les processus d'apprentissage en stimulant la plasticité synaptique (*TNT*), restaurer le sens du toucher chez des personnes appareillées (*HAPTIX*) ou permettre le contrôle de machines complexes incluant des prothèses haute performance (*Revolutionizing Prosthetics* ou *RE-NET*).

Le programme *RAM* vise à développer, à des fins thérapeutiques, une interface neurale implantable destinée à extraire des souvenirs existants, mais aussi à faciliter la formation de nouveaux souvenirs chez des personnes ayant perdu les leurs à la suite d'un traumatisme cérébral ou d'une maladie neurologique. Le programme *RAMReplay* doit quant à lui permettre d'explorer les mécanismes de mémorisation afin d'aider les personnes à se remémorer certains événements.

Le programme de R&D *NESD* (*Neural Engineering System Design*) a pour ambition de développer une interface neuronale implantable avec une résolution du signal et une bande passante sans précédent pour le transfert de données entre le cerveau et le monde digital. L'objectif est d'arriver à développer un système pouvant communiquer clairement et individuellement avec jusqu'à un million de neurones dans une région donnée du cerveau, avec un dispositif biocompatible qui ne mesurerait pas plus d'un centimètre cube et coûterait environ dix dollars. Par comparaison, les interfaces neurales qui peuvent actuellement être utilisées chez l'homme reposent sur l'agrégation de signaux provenant de dizaines de milliers de neurones, d'où des résultats imprécis. Parmi les applications potentielles figurent la possibilité de compenser des pertes auditives ou visuelles, mais également de remplacer les lunettes de réalité virtuelle et de permettre l'affichage d'informations dans le cortex visuel perceptibles uniquement par le porteur de l'implant.

Récemment, l'armée de l'air américaine a également testé l'efficacité de la stimulation transcrânienne dite « à courant direct ». Cette expérimentation a montré qu'elle améliorait la vigilance, l'attention, la mémoire de travail et la coordination motrice dans le cadre d'une opération multitâche. L'électrostimulation cérébrale pourrait ainsi présenter un intérêt pour des personnels soumis à des sollicitations multiples et devant rester concentrés sur de longues périodes, comme par exemple les pilotes de drones. Les risques d'un usage répété ne sont cependant pas connus à ce stade.

Source : op. cit.

En somme, comme le montre bien l'étude « Chocs futurs » précitée, pour autant que l'on puisse les entrevoir avec clarté à un stade aussi peu avancé de maturation technologique, le produit de la convergence entre neurosciences et numérique pourrait se traduire, pour les armées, par des applications dans les domaines suivants :

– le **suivi médical des militaires**, avec par exemple le suivi en temps réel de leur niveau d'attention ou de stress ;

– le **traitement de pathologies physiques ou psychiques résultant de blessures**, avec des systèmes de commandes par le cerveau des prothèses ou de restauration de facultés sensorielles perdues, voire de souvenirs ;

– l'amélioration de la formation et de l'**entraînement**, par exemple en situation de stress ou de fatigue ;

– **l'augmentation des performances physiques, sensorielles et cognitives** des combattants, notamment dans les environnements complexes, avec des exosquelettes ou des capteurs plus performants que les organes humains ;

– le **guidage à distance de systèmes d'armes**, robots ou drones ;

– **l'obtention d'informations et l'évaluation de leur véracité** à des fins de renseignement ;

– la **mise en réseau de capacités cérébrales** afin de pouvoir combiner des compétences individuelles.

Les rapporteurs soulignent que, **par nature, tout ce qui est possible n'est pas nécessairement souhaitable**. En effet, **les questions éthiques posées par ces éventualités scientifiques sont majeures** : comment garantir le respect de l'identité de l'homme, de son intégrité physique, et l'engagement de sa responsabilité si une machine a, en quelque sorte, pris le contrôle de son cerveau ? Si ces questions dépassent largement le champ de la mission qui leur a été confiée, les rapporteurs n'en estiment pas moins qu'elles doivent être tranchées à l'occasion d'une réflexion aussi collective que possible. Cette réflexion devra prendre en compte non seulement les impératifs éthiques qui découlent de nos valeurs, mais aussi les possibles séquelles de tels dispositifs sur les combattants ; elle devra aussi évaluer, même du point de vue éthique, une hypothèse dans laquelle certains de nos adversaires emploieraient contre nos combattants des moyens que nous ne nous autoriserions pas.

8. L'internet des objets

L'Union internationale des télécommunications définit l'internet des objets – souvent abrégé IoT, pour l'anglais *Internet of Things* – comme une « *infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* » [(1)].

(1) Union internationale des télécommunications, recommandation n° UIT-T Y.2060, juin 2012.

L'essor de ces objets connectés constitue l'une des principales tendances à l'œuvre dans le secteur des technologies numériques. Pour les représentants du SIIA rencontrés à Washington, la plus importante rupture technologique à venir dans les trois à cinq ans tient d'ailleurs à l'essor prévisible de l'internet des objets avec le déploiement de la 5G. Quant à l'étude précitée de l'*Eisenhower School*, elle donne une mesure de cet essor : on compterait 50 milliards d'objets connectés dans le monde en 2020.

Compte tenu des possibilités qu'il offre, l'internet des objets est appelé à prendre une part grandissante dans les armées, pour lesquels l'enjeu majeur tient à en sécuriser le fonctionnement.

a. L'internet des objets est appelé à prendre une place croissante dans la vie quotidienne des armées

i. Les applications multiples de l'internet des objets

Le développement d'objets connectés est pour l'essentiel le fait des entreprises civiles de haute technologie, pour des usages dont certains peuvent aisément être transposés dans les armées. Si la catégorie des objets connectés est très diverse, on peut distinguer avec une récente étude [(1)] quelques secteurs dans lesquels la croissance de ce marché est particulièrement soutenue :

– **le transport**, avec le développement de toutes sortes de capteurs permettant notamment de suivre des véhicules (autonomes ou non) voire de les piloter à distance et de mettre en œuvre des systèmes de maintenance prédictive ;

– **la logistique**, secteur dans lequel les objets connectés facilitent la traçabilité des matériels, la dématérialisation de leur documentation, l'optimisation des flux ou encore la maintenance prédictive et l'auto-réapprovisionnement ;

– **la santé**, champ dans lequel se développent à la fois des dispositifs et outils médicaux connectés (comme des capteurs de variables médicales destinés aux patients) et un large marché d'outils et d'application relevant du bien-être et des loisirs (comme les montres et bracelets connectés utilisés par les sportifs) ;

– **le bâtiment, l'énergie et la domotique**, avec l'ensemble des applications du marché dit des *Smart Home*, *Smart Buildings* et *Smart Cities*, qui permettent de gérer à distance un nombre croissant d'équipements, notamment en vue de maîtriser leur consommation énergétique ;

– **la surveillance et la sécurité**, secteur dans lequel des applications telles que les caméras à reconnaissance faciale, les capteurs de mouvement et de déplacement ou les capteurs de pression au sol connaissent un essor.

(1) Compagnie européenne d'intelligence stratégique (CEIS), Axel Dyèvre et al.*, « Internet des objets (IoT) – une nouvelle donne pour la Défense », juin 2017.*

ii. Les applications de l'internet des objets dans les armées

Les armées sont d'ores et déjà confrontées au développement des objets connectés de trois façons :

– les équipements opérationnels, proprement militaires, intègrent de plus en plus de capteurs et, comme on le verra plus loin, les systèmes d'armes tendent à s'interconnecter toujours plus étroitement, au point de former des « systèmes de systèmes » ;

– les armées s'approprient les développements technologiques civils pour leur fonctionnement courant, notamment en matière de transport et de logistique, et transposent ainsi les usages civils des objets connectés ;

– fait non négligeable, dès lors que les objets connectés se répandent dans la vie civile, **les personnels ont tendance à les utiliser (ou, à tout le moins, à les porter sur eux) pendant le temps du service**. Il en va ainsi, par exemple, des montres connectées qu'ils utilisent pour leur entraînement sportif. Cette tendance est d'ailleurs favorisée dans certaines armées et connue sous le slogan : *bring your own device* (« apportez vos appareils personnels »).

Lors de leur déplacement au 12e régiment de cuirassiers, à Olivet, les rapporteurs ont d'ailleurs pu constater que le recours à des objets connectés, notamment *via* des puces à émission radio RFID, constitue l'un des vecteurs principaux de modernisation de la logistique.

b. L'essor des objets connectés dans les armées appelle un encadrement spécifique pour en sécuriser l'usage

L'essor des objets connectés suppose un recours accru aux transmissions de données, ce qui peut présenter une double vulnérabilité : d'une part, le risque n'est pas nul de **voir certains réseaux saturés**, tant les réseaux de télécommunication du ministère des Armées sont intensivement utilisés au regard de leurs capacités. D'autre part, comme toute transmission d'information, le recours à des objets connectés expose à des **risques de détection** des signaux radio, **de brouillage** de ceux-ci, **d'interception** de l'information, voire **d'altération** de celle-ci.

Ces risques sont particulièrement prégnants pour des équipements civils utilisés tels quels par les armées ou par les militaires eux-mêmes. En effet, la cybersécurité ne fait pas l'objet des mêmes attentions dans la conception des équipements par les industries civiles que dans les programmes proprement militaires ; en outre, les fondements technologiques des objets connectés sont des standards internationaux maîtrisés par de nombreux acteurs dans le monde – comme les protocoles IP ou les liaisons *bluetooth* et *wifi* –, ce qui ne les rend que plus vulnérables. On rappellera à cet égard que récemment, la position de certaines unités américaines s'entraînant dans des bases très protégées a pu être

détectée en suivant la concentration d'utilisateurs d'une application très prisée des coureurs à pied que les militaires utilisaient sur leurs montres connectées.

En somme, même si l'utilisation de technologies civiles constitue souvent la voie la plus économique pour la numérisation des armées, des précautions restent à prendre :

– les équipements acquis par les armées méritent de faire l'objet d'une **étude systématique, même rapide, de cybersécurité**, de façon à ce que la doctrine en règle l'emploi de façon sûre ;

– rien n'interdit de donner instruction aux militaires de ne pas porter leurs terminaux numériques personnels pour certaines activités ;

– la dimension de « **cyber-hygiène** » à l'instruction et dans la formation continue mérite d'être développée. Selon le commandement du 12e régiment de cuirassiers, les règles d'usage des réseaux sociaux sont d'ores et déjà enseignées aux recrues dans le cours de leur formation initiale, rappelées avant chaque OPEX et, en tout état de cause, tous les ans. Un effort de même nature est à accomplir pour les objets connectés.

B. LES RUPTURES TECHNOLOGIQUES À VENIR CONDUISENT À TRANSFORMER L'ARCHITECTURE DE NOS SYSTÈMES D'ARMES

Tant pour exploiter le potentiel des ruptures technologiques à venir, que pour garantir la supériorité opérationnelle de nos systèmes d'armes contre des adversaires de toute nature, tirant eux aussi profit de ces avancées technologiques, la révolution numérique conduit à transformer l'architecture même de nos systèmes d'armes, qui tendent à devenir de véritables « systèmes de systèmes ».

1. Les technologies numériques ouvrent la voie au « combat collaboratif » dans les trois milieux

a. En milieu terrestre, l'opération d'ensemble SCORPION constitue la première « brique » de combat collaboratif

L'opération SCORPION vise à renouveler dans un premier temps l'ensemble du segment médian de nos équipements blindés, puis une part encore plus large des équipements de combat terrestre dans une seconde étape. Le projet de loi de programmation militaire pour les années 2019 à 2025 planifie d'ailleurs une accélération de ces programmes. Pour une présentation détaillée de l'opération SCORPION, les rapporteurs renvoient à l'avis de la commission sur les crédits relatifs aux forces terrestres inscrits au projet de loi de finances pour 2018 [(1)], qui consacre une partie détaillée à l'analyse de ces équipements.

(1) Avis n° 277, tome IV, sur les crédits relatifs aux forces terrestres inscrits au projet de loi de finances pour 2018, octobre 2017.

Le déploiement accéléré des véhicules de la gamme SCORPION marque un tournant dans l'architecture d'ensemble des parcs d'équipement terrestres, dans la mesure où, comme l'a souligné le président du GICAT, « *SCORPION repose sur le partage des informations, la mise en réseau des scénarios de riposte, la préparation automatique du système d'armes en vue de riposter si (et seulement si) le militaire le décide* ». Tel est l'objet du système d'information du combat SCORPION (SICS), qui fait l'objet d'un programme à part entière. La mise en réseau des véhicules et le partage d'informations en temps réels ouvrent ainsi la voie au « **combat collaboratif info-valorisé** », qui repose ainsi sur les capacités suivantes :

– la **radio Contact**, déployée à partir de 2019 et dont les fonctionnalités complètes permettront, à compter de 2023, de mettre en réseau l'ensemble des opérateurs d'un groupement tactique interarmes (GTIA), du fantassin débarqué au poste de commandement ;

– le **SICS**, qui, comme l'explique l'avis précité, « *permet à tous les opérateurs du GTIA de partager instantanément une carte de la zone d'opération, enrichie de diverses informations concernant l'environnement, les forces "amies" et les forces ennemies* » ;

– la « **vétronique** » de la gamme SCORPION, c'est-à-dire « *l'ensemble des capacités électroniques d'un véhicule, qui reposent sur un ensemble de capteurs – capteurs de pointage laser, capteurs de départ de missile ou de tirs – et sur un équipement de brouillage électronique des dispositifs explosifs improvisés* ».

La première étape de l'opération SCORPION prévoit la livraison de véhicules blindés multi-rôles lourds Griffon, du SICS, d'engins blindés de reconnaissance et de combat Jaguar, de véhicules blindés multi-rôles légers ainsi que la rénovation de 200 chars Leclerc. La seconde étape de l'opération doit permettre d'intégrer dans cette « bulle opérationnelle aéroterrestre » les véhicules blindés de combat d'infanterie (VBCI), les fantassins équipés du système FELIN, les véhicules blindés d'aide à l'engagement (VBAE) – successeurs des véhicules blindés légers (VBL) – ainsi que les futurs engins du génie. Différentes capacités complémentaires – tels des kits de protection active, des drones et des robots – compléteront l'équipement nécessaire au combat collaboratif.

Ainsi, pour M. Stéphane Mayer, « *SCORPION, c'est déjà de l'intelligence artificielle* », et ce système mériterait d'ailleurs d'être généralisé à d'autres plateformes d'autres milieux, comme les hélicoptères. En tout état de cause, il ressort des comparaisons internationales qu'avec l'opération SCORPION, les forces terrestres françaises disposent d'un plan d'équipement plus ambitieux que celles des autres puissances en matière d'intégration de l'ensemble des plateformes dans un système de combat collaboratif.

b. En milieu marin, l'architecture des plateformes est appelée à évoluer vers des « systèmes de systèmes »

L'étude des programmes de R&D de Naval Group a permis aux rapporteurs d'analyser les enjeux d'interconnexion des plateformes navales.

i. À court terme, des enjeux d'interconnexion des plateformes navales avec leurs futurs drones

M. Cyril Lévy, directeur des systèmes de drones de Naval Group, a expliqué que dans le milieu maritime, **les drones sont appelés à être des démultiplicateurs des capacités navales, dans une logique coopérative**.

Les **drones aériens** permettront d'étendre la capacité d'observation des plateformes navales sans exposer celles-ci au feu de l'ennemi. Ils sont ainsi appelés à embarquer dans un premier temps des moyens de renseignement, de surveillance et de reconnaissance (dits « ISR [(1)] »), et dans un second temps des armes.

Des **drones sous-marins** sont à l'étude. L'impulsion a été donnée il y a trois ans, lorsque les États-Unis ont financé pour 600 millions de dollars un programme de R&D en vue du développement d'un drone de la taille d'une torpille, capable de conduire des missions d'ISR. Les États-Unis envisagent aussi des drones sous-marins de classe océanique, qui auraient pour caractéristiques d'être autonomes et non téléopérés en permanence comme les drones aériens. Ce type de drones fonctionnera donc grâce à l'intelligence artificielle, ne serait-ce que pour l'appréciation de sa situation et l'adaptation subséquente de ses missions.

Naval Group travaille déjà sur ces briques technologiques. Les torpilles, par exemple, sont de plus en plus « intelligentes » : elles leurrent automatiquement les forces ennemies et sont capables de s'adapter de façon autonome à une évolution de la cible. L'enjeu consiste désormais à rendre ces équipements autonomes pour plusieurs jours voire plusieurs semaines.

Des **drones de surface**, principalement pour la guerre des mines, compléteront cet arsenal. Les plateformes sur lesquelles repose la guerre des mines sont en effet appelées à évoluer, pour passer des chasseurs de mines tripartites de classe *Éridan* dotés de sonars traînés à une logique de drones et de navire porte-drones. Dans ce domaine, un contrat a été attribué à Thales *via* l'OCCAr pour le compte de la France et du Royaume-Uni. Ce drone de surface pourra travailler en collaboration avec des drones sous-marins d'observation et des drones de destruction. Tel est l'objet du programme de « système de lutte antimines du futur », que confirme le projet de loi de programmation militaire 2019–2025. La première étape de ce marché, notifiée en 2014, aboutira à la livraison de deux systèmes entre 2020 et 2022. Dans une étape ultérieure du

(1) Pour Intelligence, Surveillance & Reconnaissance.

programme, seront livrés des chasseurs de mines dont la plage arrière sera adaptée pour accueillir des drones.

ii. À moyen terme, des enjeux d'interconnexion des plateformes navales entre elles

M. Philippe Méléard, directeur de l'architecture des « systèmes de systèmes » de Naval Group, a expliqué que cette architecture consiste à « ***raisonner en "système de combat de la force navale" aéromaritime*** », ce qui suppose :

– de mettre en réseau les différents navires armés ;

– de fournir des incréments rapides des systèmes de chaque navire armé ;

– de développer des partenariats stratégiques de nature à assurer une supériorité technologique et opérationnelle à la force d'action navale.

Il a expliqué que la menace principale pesant sur nos plateformes navales étant les missiles, et cette menace progressant très vite, la réponse à celle-ci « *ne pourra être qu'automatique* », et l'alerte doit être la plus précoce possible. Répondre à cette menace suppose donc de **mettre en réseau l'ensemble des capteurs et des effecteurs** de la force navale. Ainsi, l'interconnexion des plateformes est la clé de la réactivité de la force, et s'avère particulièrement nécessaire face aux stratégies de saturation : « *détecter et cibler un missile unique n'est pas la même chose qu'une myriade de vecteurs* ».

La **gestion des flux d'information**, que ce soit en temps « réel » ou en temps « réfléchi », constitue un enjeu majeur de la mise en réseau des informations. Certes, les débits des transmissions peuvent augmenter, par exemple avec le lancement prochain du satellite Syracuse IV ; mais la redondance étant la règle, il faut pouvoir se contenter aussi de systèmes moins puissants, comme la radio à très haute fréquence. La R&D de Naval Group en la matière a abouti à la définition de l'architecture numérique de la FTI, qui règle le stockage et la gestion des données, que ce soit de temps réel (*via* un *data center*) ou réfléchi, *via* des dispositifs dits de C3I (pour *Command, Control, Communication, Intelligence*). Ces développements sont appelés à se poursuivre pour donner corps, en plusieurs étapes d'incrémentation, à une « **capacité d'engagement coopératif** » complète.

Les rapporteurs se sont aussi fait présenter la plateforme d'intégration, de validation et de certification du système de direction de combat (***Combat Management System***, **CMS**) d'une FREMM. Il en ressort que lorsque le radar de la frégate observe des objets volants, les systèmes d'information tactiques permettent de l'analyser et, si le vecteur aérien en question est identifié comme menaçant, de le cibler en temps réel en pointant sur lui un missile. La machine peut identifier un vecteur ennemi sur la base de catalogues d'identification des vecteurs. C'est cependant un opérateur humain qui doit ordonner le tir, mais la technologie permettrait d'ores et déjà des tirs automatiques. En cas de détection

d'un nombre d'objets tel que les capacités de traitement simultané des cibles seraient dépassées, le système peut établir lui-même des ordres de priorités entre les cibles. Ce système témoigne de l'intégration réussie de capteurs (tels les radars) et d'effecteurs (notamment des missiles). Interconnectant une interface en temps réel et des outils fonctionnant en temps « réfléchi », il constitue un véritable **système de combat collaboratif**.

c. En milieu aérien, le système de combat aérien futur repose sur la mise en réseau des appareils

i. L'interconnexion des plateformes, une stratégie permettant de gagner en efficacité opérationnelle sans sacrifier le volume des forces

La mise en réseau des plateformes aériennes est désormais conçue comme le principal moyen à la portée de l'armée de l'air pour garantir dans la durée sa supériorité opérationnelle face aux menaces actuelles. Comme l'a expliqué la commissaire générale Françoise Latour, chargée de mission sur la transformation numérique à l'état-major de l'armée de l'air, pour le système de combat aérien futur (SCAF), garantir la supériorité aérienne à l'horizon 2030 suppose de « ***sortir d'une logique de plateformes individuelles au profit d'une logique de système global*** ».

En effet, l'avantage opérationnel des forces aériennes occidentales se réduit sous les effets conjugués de trois facteurs :

– une augmentation de la menace dite de « haut du spectre », notamment avec les capacités de déni d'accès reposant sur des systèmes de défense anti-aériennes intégrées, de très longue portée, comme les batteries de S300 et S400 déployées en Syrie ;

– des acteurs non étatiques qui utilisent des modes d'action asymétriques et ont recours « *à des armes à bas coût et à des technologies faciles d'accès permettant d'amoindrir l'avantage technologique occidental : mini-drones, engins explosifs improvisés,* smartphones*, propagande* via *les réseaux sociaux* » ;

– le développement de technologies susceptibles de contribuer à remettre en cause les rapports de force actuels, comme l'intelligence artificielle, le développement des drones, les progrès dans les technologies de détection, ou encore l'hypervélocité des missiles.

Concernant les menaces de « haut du spectre », selon la commissaire générale Françoise Latour, « *le chef d'état-major de l'armée de l'air constate que les arsenaux aériens et anti-aériens de nos adversaires potentiels, mais aussi de nos partenaires, ont tous fait des efforts de modernisation* » et que « *retarder notre modernisation nous fait courir un réel risque de déclassement stratégique* ». Si certains de nos alliés se sont engagés dans l'acquisition d'appareils de nouvelle génération avec le programme de F35, elle a souligné que le coût de ce programme est tel qu'il risque de contraindre les armées dont le budget n'est pas

extensible *ad nutum* à arbitrer entre avancée technologique et volume de forces, en défaveur de ce dernier. Schématiquement, l'avion de nouvelle génération coûtant plus cher que le précédent, certains pays en acquerront un nombre inférieur à celui de leurs flottes actuelles. Or il y a une limite à cette logique, c'est-à-dire un volume de forces en deçà duquel il est déraisonnable de réduire la taille d'une armée.

Concernant des acteurs moins avancés en technologies, comme nos adversaires au Sahel, elle fait observer que compte tenu de l'étendue des théâtres, « *les résultats opérationnels ne peuvent y être l'œuvre d'un seul avion ou d'un GTIA, même individuellement performants* ». Au contraire, « *les succès que nous obtenons là face aux groupes terroristes sont le résultat d'une combinaison de modules de forces interarmées, déjà connectés entre eux et réarticulés en fonction de la situation : drones, avions de chasse, de transport et de renseignement, forces spéciales, hélicoptères de transport ou de combat, et bien sûr centres de commandement au sol partageant le flux d'information en temps réel* ». Ce dispositif peut ainsi concentrer dans une fenêtre de temps extrêmement étroite une combinaison des effets pour trouver, traquer et affronter l'ennemi.

La commissaire générale Françoise Latour a donc présenté l'interconnexion des plateformes aériennes comme une stratégie capacitaire permettant de répondre à l'intensification de l'ensemble de ces menaces par des moyens permettant de réduire la « boucle de décision », c'est-à-dire d'accroître la réactivité des forces. En effet, **l'interconnexion des plateformes par l'exploitation des technologies numériques** peut augmenter l'efficacité collective des plateformes aériennes. L'intelligence artificielle y contribue, pour des fonctions d'aide à la décision. La mise en réseau des capteurs et des effecteurs doit ainsi permettre de « *compenser un éventuel et léger décrochage technologique* ». De même, l'accroissement de la réactivité des forces par leur interconnexion constitue la clé du combat contre des groupes armés terroristes agiles et prompts à « se fondre » dans leur environnement.

ii. Une stratégie qui détermine l'architecture de nos plateformes aériennes, à commencer par le système de combat aérien futur

Selon l'état-major de l'armée de l'air, les réflexions engagées sur le SCAF conduisent à concevoir ce système de combat comme « ***une combinaison de moyens humains, physiques, réseaux et logiciels*** *: plateformes pilotées, drones téléopérés, moyens spatiaux, armements, centres de commandement et de conduite, capteurs et forces au sol et en mer connectés les uns aux autres, réseaux et systèmes d'information* ».

La nouveauté, dans cette optique, tient à ce que « *plutôt que de penser d'abord les plateformes pour les connecter ensuite entre elles* » – ce qui *a posteriori* ne manquerait pas d'être difficile et coûteux –, l'armée de l'air est attachée à ce que « ***l'architecture globale du système et en particulier le réseau aéronautique de communications pour le combat qui sous-tendra la connectivité***

***d'ensemble soit organisés* a priori** ». Dans ce système, l'information – c'est-à-dire les données numériques –, doit être « *à la base de la réflexion, pour définir l'architecture du futur C2 de l'ensemble* ». Grâce à l'apport des nouvelles technologies du numérique – comme le *big data* ou l'intelligence artificielle –, l'enjeu est de « *créer un système ouvert et collaboratif* », capable de collecter et stocker des quantités très importantes de données, de les protéger, de les échanger, de les fusionner et de les distribuer de façon intelligente et dynamique. La commissaire générale Françoise Latour a appelé ce concept : « *Data to Decision* ».

Ainsi, **la numérisation est vue comme la colonne vertébrale du système de combat aérien futur car elle permet l'interconnexion des plateformes**.

D'ailleurs, l'armée de l'air s'attache à ce que les « briques » fondamentales du SCAF en matière de transmissions soient incluses dans les programmes de rénovation ou les nouveaux programmes lancés à court terme, comme le passage du Rafale au standard F4, la charge universelle de guerre électronique (CUGE) ou le standard 2 de l'avion ravitailleur MRTT. En effet, une fois les équipements de connectivité installés, ajouter un système de traitement de l'information par exemple utilisant l'intelligence artificielle ne sera pas excessivement complexe et ne nécessitera pas une rénovation majeure.

Ainsi, le SCAF ne sera donc ni un avion ni un drone, mais « *un ensemble de systèmes connectés, agiles, redondants, ouverts et sécurisés* », qui constitueront l'architecture de l'aviation de combat du futur et qui, plus que d'additionner simplement les performances individuelles des plateformes, permettra d'en multiplier les effets.

d. Un effort commun à l'ensemble des milieux d'opération : la maîtrise de l'architecture des systèmes de défense

L'amiral François Moreau a bien souligné qu'au-delà de l'interopérabilité des équipements appartenant à une même armée, l'interconnexion des plateformes revêt nécessairement une dimension interarmées. La marine nationale y est particulièrement sensible. En effet, les marins étant engagés dans les trois milieux d'opérations, il convient de veiller à ce que leurs équipements soient interopérables avec les outils « métier » des autres armées, notamment ceux qui sont développés sous forme de modules « métier » greffés au système d'information des armées (SIA). À titre d'exemple, tout module développé par l'armée de l'air pour le combat aérien intéresse l'aéronautique navale. De même, tout ce qui concerne le développement d'outils de renseignement interarmées, au niveau stratégique, intéresse aussi chaque armée au niveau tactique.

Dans cette optique, la DGA et l'état-major des armées se sont engagés dans une démarche d'ingénierie visant à assurer la **maîtrise de l'architecture des systèmes de défense** (**MASD**). Comme l'a expliqué chez Naval Group M. Philippe Méléard, cette entreprise se décline en cinq volets, correspondant aux trois milieux classiques d'opération, au champ de la « surveillance, l'acquisition,

la reconnaissance et le renseignement », ainsi qu'à la cyberdéfense. Elle vise à **rationaliser progressivement les architectures des systèmes des différentes plateformes, afin de garantir leur cohérence**. Il s'agit ainsi de raisonner de façon transversale, en concevant les plateformes en termes de réseaux, plutôt qu'autour d'une plateforme unique (par exemple, entre le porte-avions et l'avion).

La conception d'une telle architecture « *dépend, bien entendu, d'une vision prospective à l'horizon d'une trentaine d'années* ». Des études technico-opérationnelles sont prévues pour y pourvoir, et des projets de science et de technologie permettront d'évaluer le potentiel de différentes technologies.

2. Le « déluge d'informations » rend indispensables les technologies de traitement automatisé des données

a. Dans les forces, la masse des informations disponibles ne pourra être pleinement exploitée que par des systèmes d'aide à la décision

Comme le dit le rapport précité de notre collègue Cédric Villani, le volume de données produites croît exponentiellement, la précision et la granularité des données produites par les capteurs augmentent et cette tendance ne va que s'accentuer avec le temps, si bien qu'« *avec les ressources humaines disponibles, quand aujourd'hui on parvient à traiter une quantité de données qui avoisine au mieux les 20 %, à terme ce sera probablement moins de 2 %* ».

Pour endiguer ce phénomène, il est donc nécessaire à ses yeux « *que les investissements réalisés dans le domaine des capteurs aillent de pair avec ceux dans l'intelligence artificielle permettant d'en exploiter la production* ». Cependant, bien loin de rendre automatique la prise de décision, « *il s'agit avant tout de permettre à des opérateurs d'appréhender, de naviguer dans et d'exploiter la masse de données* ». L'intelligence artificielle offre ici « *de nouvelles perspectives* » ; en effet, ces technologies permettent de mieux exploiter à la fois les données produites en continu, mais aussi « *le patrimoine amassé* ».

Ainsi, l'intelligence artificielle peut servir à traiter des informations pour les présenter de façon claire et intelligible à l'humain chargé de prendre une décision, qu'il s'agisse d'un pilote dans son cockpit, d'un chef tactique au sol, d'un chef opératif ou des plus hautes instances de la chaîne de planification et de commandement des opérations.

b. Dans les services de renseignement, les ruptures technologiques à venir permettront d'améliorer le traitement automatisé des données

On l'a dit, le volume de données que les services de renseignement sont à même de capter est tel que les moyens humains ne suffisent pas à son exploitation.

Tel est l'objet du programme ARTEMIS susmentionné. Dans le cadre de cette démarche, un programme d'études amont (PEA) a été lancé, et un premier démonstrateur devrait être disponible en 2020 ; les « briques » de systèmes

d'information de chaque service de renseignement y seront alors intégrées progressivement. L'échéance du projet est envisagée pour 2026. L'équipement ARTEMIS devra posséder une architecture assez souple pour connaître des évolutions futures et, d'emblée, intégrer des « briques » logicielles supplémentaires.

Outre les outils de *big data* évoqués précédemment, d'autres technologies numériques pourraient contribuer à accroître leur efficacité. Ainsi, le directeur du renseignement militaire a jugé indispensable d'innover, en tirant parti des possibilités que l'on entrevoit des **technologies d'intelligence artificielle**. Ces développements pourraient par exemple être conduits par des incréments éventuels du programme ARTEMIS décrit plus haut. Dans ce type de projets, l'expression des besoins est particulièrement complexe, du fait de l'évolution rapide des technologies ; comme le dit le général Jean-François Ferlet, « *il y a cinq ans, on imaginait à peine les outils que nous utilisons aujourd'hui* ».

Dans son rapport, notre collègue Cédric Villani met d'ailleurs en avant l'exemple suivant, qui intéresse au premier chef les services de renseignement : « *dans la recherche de contenu dans un ensemble de vidéos, quand il aurait précédemment fallu faire visualiser ces vidéos minute par minute par un ensemble d'opérateurs humains, il est aujourd'hui envisageable d'utiliser des techniques d'intelligence artificielle pour faire ce travail de façon automatique et beaucoup plus rapide* ».

3. Les transmissions prennent une importance cruciale

L'exploitation des technologies numériques et la mise en réseau accrue des équipements avec la généralisation de « systèmes de systèmes » rendent les transmissions particulièrement cruciales. Or celles-ci sont également appelées à connaître des évolutions avec les progrès technologiques à l'œuvre. Sans entrer ici dans un exposé détaillé des différents programmes de télécommunications, les rapporteurs tiennent à mettre en exergue, d'une part, les possibilités offertes par le concept de « *cloud* de combat » (*combat cloud*) et, d'autre part, les enjeux nouveaux qui s'attachent aux équipements spatiaux.

a. Le « cloud de combat », infrastructure de partage d'information adaptée au combat collaboratif

La mise en réseau des plateformes et des hommes suppose une infrastructure de partage de données de plus en plus complexe à mesure que croissent le volume des informations à partager et le nombre de plateformes, de centres de commandement et d'hommes qui y sont connectés. Dans la lignée des programmes en cours, c'est vers une sorte de « *cloud* de combat » – on parle aussi de « *cloud* tactique » ou de « *cloud* de théâtre » – que paraît s'acheminer l'architecture de ces systèmes d'information.

i. La transformation en cours des infrastructures de partage de l'information opérationnelle

Comme on l'a vu, les programmes de renouvellement de nos principales plateformes font une large part aux systèmes d'information opérationnels et de communication (SIOC) qui sous-tendent la mise en réseau des capteurs et des effecteurs, au moins au niveau tactique. Le SICS est emblématique de cette évolution. Au niveau stratégique et à l'échelon opératif, le programme de système d'information des armées concourt au même objectif, en unifiant progressivement les systèmes d'information de chaque armée.

C'est en effet la performance de l'infrastructure de partage de l'information qui permet de raccourcir la boucle de décision et de conférer ainsi aux forces la réactivité nécessaire à la supériorité opérationnelle.

ii. Une transition vers le *cloud* à l'œuvre parmi d'autres forces

- *Une technologie privilégiée par des puissances occidentales*

Confrontées aux mêmes défis, d'autres armées se sont résolument orientées vers le développement de systèmes de *cloud*. Tel est le cas, par exemple, aux États-Unis. Les rapporteurs se sont ainsi fait présenter à Washington les axes de R&D poursuivis en la matière par *Amazon Cloud Services*, qui semble s'imposer comme le fournisseur de référence du *Department of Defense* pour les technologies de stockage et de gestion de données en ligne, *via* le *cloud.*

Il faut d'abord distinguer, dans le *cloud*, capacité de stockage et capacité de calcul. Selon les responsables d'*Amazon Web Services*, « *le stockage est une chose, mais* ***le*** **cloud** ***permet bien d'autres usages dès lors qu'il est vu plus largement comme une base technologique pour des applications*** ». D'après elles, les discussions sur le *cloud* entre *Amazon* et le *Department of Defense* tournent désormais moins autour du stockage des données qu'autour de l'intelligence artificielle qui peut y être associée, par exemple en matière de reconnaissance faciale ou de *big data*. « *Les technologies actuelles auraient permis, selon le secrétaire d'État à la Défense James Mattis, d'"attraper" Edward Snowden.* »

Les applications possibles sont en effet nombreuses ; la reconnaissance faciale *via* les caméras de surveillance peut être opérée par des applications placées directement sur le *cloud* ; des usages prédictifs sont également possibles, par exemple en matière de météorologie. *Amazon* considère ainsi que **les technologies de *Machine Learning* et d'intelligence artificielle sont d'autant plus efficaces qu'elles reposent sur le *cloud***.

Pour *Amazon*, la création en 2017 d'un *Department of Defense Cloud Executive Steering Group* (1) traduit à cet égard un changement de cap du ministère

(1) Comité directeur du cloud *du Département de la Défense.*

en faveur du *cloud*, dont l'encadré ci-après présente certaines traductions concrètes.

La transition des armées américaines vers le *cloud*

M. Randall Conway, adjoint à la *Chief Information Officer* (CIO) du Pentagone en charge de la gestion de l'information du ministère (*Information Enterprise*), c'est-à-dire la direction stratégique et le contrôle de l'environnement informatique interarmées (*Joint Informational Environment*), a présenté en détail plusieurs chantiers actuels conduits par son service, lesquels reposent pour une large part sur l'utilisation du *cloud computing*, notamment dans le champ opérationnel. On retiendra :

– la fourniture aux forces américaines de systèmes d'information dédiés spécifiquement à la coopération avec les alliés des États-Unis. Ces systèmes reposeront sur **six *data centers* virtuels, hébergés sur un système de *cloud* du *Department of Defense*** ;

– l'optimisation des infrastructures de données, qui consiste notamment à mettre en œuvre la **transition des données vers des *clouds*** ;

– la fourniture aux forces de produits facilitant leur mobilité, tels que des réseaux de connexion sans fil (*wifi*) ou des terminaux mobiles, permettant d'accéder à des informations à distance et d'en transmettre, dans une logique d'interconnexion des capteurs et des effecteurs autour d'un *cloud* de combat ;

– le projet de « *Joint Regional Security Stack* », qui consiste en un ensemble d'équipements assurant les fonctions de pare-feu, de prévention et de détection des intrusions, de routage et d'adressage de données et de diverses autres fonctions ayant trait à la sécurité des réseaux. Son intérêt tient à son caractère centralisé : au lieu que les équipements de sécurité soient répartis dans chaque implantation des forces armées, ils seront regroupés au sein d'architectures informatiques régionales. Ce système permettra de graduer le niveau de sécurité en fonction du niveau de classification des informations qu'il traitera – à l'exception du « *top secret* », qui relève d'autres réseaux. Ces équipements, tous issus de l'industrie civile, comportent aussi des applications d'analyse de données.

La *Defense Information Security Agency* (DISA) [(1)] n'étant pas en mesure de fournir le même niveau de service de *cloud computing* que l'industrie privée, le *Department of Defense* a choisi de lancer un **appel d'offres pour cinq milliards de dollars** environ, visant au développement d'un système de *cloud* accessible pour quatre millions d'utilisateurs. Le déroulement du marché est prévu selon une logique incrémentale : il est prévu de développer le *cloud* d'abord pour des données non classifiées – ce qui ne les empêche pas d'être sensibles, donc protégées – et d'en venir, le cas échéant, à des niveaux de plus en plus élevés de classification. Si les développements récents de l'actualité ont vu le Pentagone remettre à plus tard la réalisation du projet d'équipement pour lequel cet appel d'offres a été passé, pour des raisons qui pourraient tenir à l'application de règles de concurrence, rien n'indique pour autant qu'il ait renoncé à son projet.

- *Une technologie utilisée aussi par nos adversaires*

Certaines applications civiles largement répandues reposent sur des technologies de transfert sécurisé de données, à partir de terminaux de la gamme commerciale *via* les réseaux civils de télécommunications, en vue de leur stockage, de leur traitement par des applications installées sur des serveurs

(1) Agence de sécurité de l'information de la Défense.

distants, et de leur partage. Il s'agit donc là de technologies de *cloud computing*. Tel est le cas, notamment, de services de messagerie.

Or il est avéré que certaines organisations terroristes, comme Daesh, utilisent de telles applications – comme la messagerie *Telegram* – au service de leurs funestes desseins. Ainsi, certains de nos adversaires exploitent déjà la réactivité de ces technologies de *cloud* pour des fonctions que l'on pourrait dire de commandement et de conduite d'opérations. Elles leur permettent de mettre en réseau leurs personnels avec une grande réactivité, qui constitue ainsi un défi pour nos propres forces.

iii. Des réflexions et des développements conduisant à la mise en place d'un véritable « *cloud* de combat »

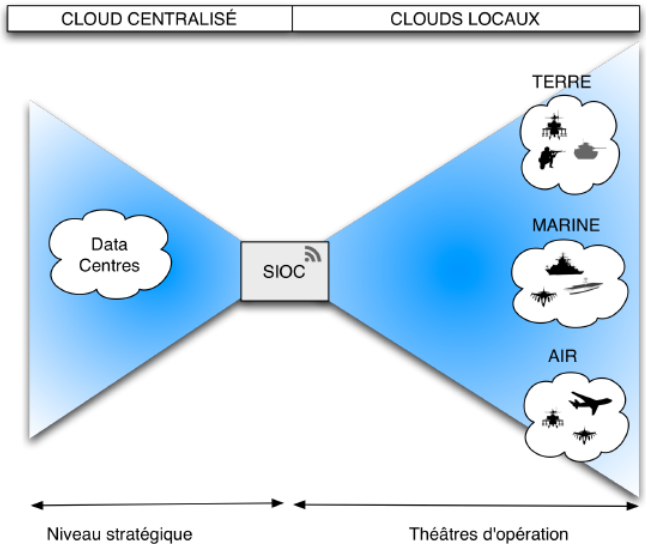
Avec l'entrée en service de nouvelles générations de plateformes plus « communicantes » que les précédentes, le concept de « *cloud* de combat » fait l'objet d'études poussées. Les réflexions actuelles s'orientent autour d'un **système de *cloud* dit hybride**, c'est-à-dire articulant :

– des données stockées à des échelons décentralisés de la chaîne de commandement afin d'en garantir l'accès en cas d'indisponibilité ou d'insuffisance de débit des réseaux, que ce soit à l'échelon opératif ou au niveau tactique, voire dans les mémoires des terminaux faisant partie de l'équipement individuel du militaire ou de la plateforme qu'il opère ;

– des données stockées hors des zones d'opération et accessibles par un *cloud*, ce qui permet de s'affranchir des limites de capacité de stockage des équipements individuels et de partager, éventuellement en temps réel, des masses d'information conséquentes.

Ainsi, les SIOC pourraient assurer une interface entre des données stockées au niveau stratégique et les *clouds* déployés aux niveaux opératif et tactique, le cas échéant par armée. Le schéma ci-après illustre cette idée d'architecture.

UN « *CLOUD* DE COMBAT »



Source : Compagnie européenne d'intelligence stratégique (CEIS), Axel Dyèvre et al.*, « Emploi du cloud dans les armées – Première approche des concepts et contraintes », août 2016.*

iv. Des applications particulières pour les services de renseignement

Les entretiens des rapporteurs avec Mmes Maria Saab, Erica McCann et Iram Ali, représentantes d'*Amazon Web Services*, ont permis d'étudier les moyens fournis par cette société à la communauté américaine du renseignement en matière de ***cloud computing***. Le gouvernement américain a en effet eu recours aux prestations d'*Amazon* plutôt qu'aux capacités de développement internes de ses services pour mettre en place le service de *cloud computing* commun des dix-sept agences et services formant la communauté américaine du renseignement.

Un effort de partage d'informations entre les différents services de renseignement a été érigé en priorité par les plus hautes autorités politiques américaines après le 11 septembre 2001. Le *cloud* s'est alors imposé comme la technologie de référence en la matière.

C'est ainsi que les services de renseignement ont choisi en 2006 de passer un contrat dit C2S – pour *Commercial Cloud Service* [(1)] – en vue de remplacer les systèmes informatiques propres à chacune des agences concernées, reposant sur des *data centers* cloisonnés. Un premier contrat a été attribué en 2006 à IBM, qui, selon les responsables d'*Amazon Web Services*, « *était alors la seule entreprise dont les employés disposaient des habilitations nécessaires* ». En 2014, le contrat C2S a été attribué à *Amazon Web Services*, et « *ce programme d'équipement a pris en importance* » : il a été conclu pour 600 millions de dollars, avec des options dont l'activation a porté le montant à un milliard de dollars.

(1) Service de cloud *issu de la gamme commerciale.*

Amazon a ainsi créé une *Intelligence Community Market Place*. Il s'agit d'une sorte de catalogue de logiciels et d'informations à la disposition directe de tous les services et agences de renseignement américains, ce qui leur évite de passer chacune « *par des procédures d'acquisition lourdes, longues et donnant souvent lieu à des sur-spécifications* ». *Amazon Web Services* a financé cet outil sur fonds propres – pour un montant qui n'a pas été précisé – et reste propriétaire de son infrastructure informatique ainsi que responsable de ses employés la mettant en œuvre. Le *hardware* est ainsi standardisé.

Bien entendu, le choix de telle ou telle solution technique, plus ou moins intégrée, doit être déterminé par l'état de la législation en matière de partage des informations entre services de renseignement. Néanmoins, rien n'interdit de penser que des applications de gestion des droits d'accès permettraient de mettre en œuvre dans un *cloud* les limites fixées par le droit, tout en garantissant une certaine souplesse et une certaine réactivité dans le partage légal des informations et en exploitant les possibilités de traitement des données en ligne.

b. Les équipements spatiaux, plus nécessaires et plus vulnérables qu'auparavant

L'interconnexion des différentes plateformes et la constitution de « bulles » d'information autour des unités déployées reposent en partie sur des moyens de télécommunication satellitaire. En outre, la planification et la conduite des opérations reposent sur l'exploitation de masses de renseignements de toute origine, provenant pour une part de satellites. Ainsi, la numérisation croissante du combat accroîtra assurément notre dépendance aux moyens satellitaires.

Celle-ci est d'ores et déjà marquée. Le général Jean-Pascal Breton, commandant interallié de l'espace, en a donné la mesure devant la commission [(1)] :

– en 2016, les armées ont acquis 45 883 images prises par des satellites, ce nombre allant croissant d'année en année ;

– les forces ont déployé quatre-vingt-treize stations de télécommunication par satellite, dans tous les endroits du monde où elles sont engagées ;

– quasiment toutes les missions conduites par les forces françaises ont utilisé le GPS ; tel est aussi le cas des deux tiers des armements tirés.

Ainsi, « ***les télécommunications satellitaires sont une capacité clé de l'autonomie de décision et d'action de nos forces armées*** », notamment du fait de l'extension continue de nos théâtres d'opérations, qui impose de trouver des moyens de communication de longue distance entre Paris et ces zones.

(1) Assemblée nationale, commission de la Défense nationale et des forces armées, réunion du 20 décembre 2017, audition du général Jean-Pascal Breton, commandant interarmées de l'espace, compte-rendu n° 24.

Cette dépendance croissante comporte deux défis :

– l'un, d'ordre quantitatif, consiste à fournir aux armées des débits de données répondant à leurs besoins croissants ;

– l'autre, d'ordre davantage qualitatif, consiste à sécuriser les moyens spatiaux de captation et de transmission d'information contre les risques de captation des informations ou de compromission de leur intégrité, voire de destruction physique des satellites – qu'elle soit accidentelle, liée aux débris spatiaux, ou délibérée, dans un contexte où l'espace devient, aux termes du général Jean-Pascal Breton, « *un champ de confrontation à part entière* ».

Il y a donc lieu de se féliciter de ce que **le projet de loi de programmation militaire pour les années 2019 à 2025 prévoit de renforcer nos capacités spatiales de télécommunications**, et ce à deux égards :

– la programmation proposée prévoit le remplacement avant 2025 de nos satellites SYRACUSE III [(1)] par des satellites de nouvelle génération, appelée SYRACUSE IV à propulsion électrique, opérant en bandes X et Ka dont la cybersécurité sera renforcée et qui seront rendus plus résistants au brouillage ;

– elle prévoit aussi l'augmentation du format de cette capacité, avec la livraison d'un troisième satellite SYRACUSE IV d'ici à 2030, en sus des deux initialement prévus.

4. La place de l'homme dans le combat évolue à l'ère de la numérisation

Les promesses de progrès technique que portent les développements des technologies numériques pour nos armées suscitent en contrepoint des interrogations sur la place de l'homme dans le combat futur. Schématiquement, si l'intelligence devient artificielle et si les tâches les plus dangereuses peuvent être confiées à des robots ou à des drones, quelle place reste-t-il à l'homme, au soldat ? Peut-on, de façon conforme à nos valeurs, laisser des machines prendre des décisions engageant la vie ou la mort ?

Les rapporteurs considèrent qu'une réflexion sur la place de l'homme dans le combat numérisé fait pleinement partie des enjeux de la numérisation des armées. Cette réflexion mérite d'être nourrie pas différentes approches – juridiques, éthiques, voire philosophiques, mais aussi techniques, tant il est vrai que de tels sujets peuvent nourrir des fantasmes relevant davantage de la science-fiction que de l'art de la guerre. Ils entendent donc y apporter leur contribution, sans prétendre épuiser à eux seuls l'ensemble des dimensions de la question.

Nécessairement, la perspective d'armement des drones et, de manière plus générale, la possibilité technique d'une ouverture automatique du feu, amènent à se poser la question de la place de l'homme dans la boucle d'engagement du tir.

---

(1) SYstème de RAdiocommunication Utilisant un SatellitE.

Les rapporteurs soulignent que si cette question pourrait susciter des réflexes défavorables pour des raisons d'ordre éthique, elle doit être prise dans sa globalité et dans toute sa complexité, technologique comme éthique. En effet, si l'on n'admet guère volontiers la possibilité – toute théorique – qu'une intelligence autre qu'humaine puisse être conduite à décider l'ouverture du feu, **serait-il pour autant éthique d'exposer nos propres soldats à des armements automatisés ?**

Si, face à un système d'armes adverse automatisé ou réalisant des attaques de saturation, seul un système automatisé était capable de se défendre à temps et de survivre, la question de l'ouverture du feu de manière automatique ou systématique face à des cibles incertaines et dans un environnement non maîtrisé se pose. Elle ne saurait être résolue « à la hussarde », par la négative absolue. Elle trouvera sa réponse dans un travail de doctrine établissant à quelle place intervient l'homme dans l'ouverture du feu et le contrôle des armes tirées, **à titre offensif ou défensif**.

a. Les armées opèrent d'ores et déjà nombre d'équipements dotés d'automatismes

Les applications envisageables de l'intelligence artificielle et de la robotique constituent-elles véritablement une révolution ? Une étude approfondie des technologies actuelles conduit à relativiser la portée de la rupture – au moins du point de vue de la place de l'homme « dans la boucle » –, dans la mesure où les armées opèrent d'ores et déjà des systèmes automatisés, même en matière d'armes.

En effet, sur les frégates de défense aérienne par exemple, des systèmes de lancement automatique existent depuis les années 1990, tant pour les brouilleurs que pour les missiles eux-mêmes. Néanmoins, conformément à la doctrine actuelle, **le commandant conserve « *une sorte de "droit de veto"* »**. C'est ainsi que la marine nationale veille à ménager des dispositifs garantissant l'intervention de « l'homme dans la boucle ». Ainsi, « *on est loin du "robot tueur autonome"* », dans la triple mesure où le système d'information sur lequel repose un automatisme demeure **paramétré par un humain** qui fixe des règles, où le **mode « automatique » est toujours enclenché par un homme**, et où un homme peut à tout moment « ***appuyer sur le bouton rouge*** » lorsqu'est employé un système numérique.

M. Éric Trappier, président du GIFAS, a d'ailleurs indiqué que lors du développement du Rafale, « *les pilotes refusaient tout système automatique outrepassant leurs ordres en cas de risque de crash ; ils y sont venus* ». D'ailleurs, d'ores et déjà, le lancement des leurres à bord des avions est automatique.

De plus, comme l'a fait valoir la commissaire générale Françoise Latour, la question de savoir s'il est **éthiquement acceptable de combattre et de tuer sans être soi-même en situation de danger physique** « *a déjà été tranchée car elle* ***concerne aussi le sniper, l'artilleur, le pilote de bombardement, les tirs de***

missile de croisière depuis les Rafale ou les sous-marins ». Quant aux drones, l'état-major de l'armée de l'air souligne que « ***s'il n'y a personne à bord d'un drone, il reste téléopéré par un équipage*** » constitué d'un pilote et de trois spécialistes capables de prendre des décisions en liaison avec l'état-major de théâtre.

Certes, les technologies actuelles permettent d'envisager des équipements autonomes, disposant d'une capacité d'apprentissage, et plus seulement des équipements automatiques. Mais, dès lors qu'ils restent conçus, programmés et mis en œuvre par un homme, et qu'un homme peut en reprendre le contrôle, cette évolution technologique ne conduit pas nécessairement à une rupture dans la place de l'homme « dans la boucle » de décision. C'est en ce sens que le sous-chef d'état-major de la marine nationale chargé des plans et des programmes a estimé que « *l'autonomisation n'est plus un tabou* ».

b. La rupture technologique à venir ne doit pas être exagérée

Les représentants d'IBM avancent en outre que loin de déposséder l'homme de son rôle dans la conduite des opérations, **le recours à l'intelligence artificielle permettra au contraire de maintenir « l'homme dans la boucle »**, et « *d'y maintenir même* ***davantage d'humains au bon niveau d'information*** ». En effet, le raccourcissement des délais de traitement et d'analyse des données permettant de diffuser la même information en même temps à tous les échelons de commandement, « *le lien entre échelons tactique et stratégique s'en trouve resserré* ». En somme, l'automatisation ne pose guère de problèmes en matière d'auto-défense ; mais pour des actions offensives, l'enjeu se borne à raccourcir le circuit de décision, à l'échelle du système de C2 entier, dans lequel une autorisation de tir prend beaucoup de temps.

D'ailleurs, comme le souligne le rapport de notre collègue Cédric Villani, les principaux développements qui impliquent des techniques d'intelligence artificielle « ***portent sur l'aide à la décision et à l'exécution plutôt que sur sa substitution*** ». En effet, ils visent à « *décharger les opérateurs humains de tâches chronophages et à faible valeur ajoutée* » pour leur permettre de se concentrer sur leurs missions à plus haute valeur ajoutée.

Il n'est d'ailleurs pas certain que l'intelligence artificielle puisse jamais atteindre le même degré d'autonomie que l'homme dans la décision. Comme le dit à ce propos notre collègue Cédric Villani, pour cela, « *il faudra une rupture technologique qui n'a pas encore eu lieu aujourd'hui* », soulignant que « *pour beaucoup d'experts* », une telle rupture est d'ailleurs « ***encore lointaine et peu crédible*** ». Pourtant, relève-t-il, c'est ce niveau d'autonomie qui semble être le sujet de préoccupations majeures de la population. Aux yeux des dirigeants de l'INRIA, « *voir l'intelligence artificielle comme prenant le pas sur l'être humain reste un fantasme : on est extrêmement loin d'une intelligence collective* ».

Il serait certes hasardeux, du point de vue strictement scientifique, de soutenir que l'humain est toujours plus fiable que l'informatique : pour nombre d'observateurs, les avions sont au contraire plus fiables depuis que leur pilotage ne repose plus seulement sur les humains. Mais les systèmes existants sont très spécialisés : ils peuvent être compétents, mais pas toujours plus que l'homme, et jamais dans un large champ d'activité. Surtout, pour M. Antoine Petit, « ***le vrai risque avec les armes automatiques n'est pas la prise de pouvoir des machines sur l'homme, mais le*** **bug** ». Les briques d'analyse logicielle concernées reposent en effet sur des statistiques, et ont des marges d'erreur.

En tout état de cause, fait valoir M. Éric Trappier, même avec l'intelligence artificielle appliquée aux systèmes d'armes, **l'homme aura toujours sa place, mais pas nécessairement la même qu'aujourd'hui** : ne serait-ce que la programmation des algorithmes au moins et le contrôle des feux ne sauraient relever que de lui. Ainsi, **la machine ne prendra pas le contrôle sur l'homme, ne serait-ce que parce qu'elle est programmée par l'homme**.

Il faut souligner de surcroît que les recherches actuelles portent bien davantage sur des systèmes hybrides, c'est-à-dire des systèmes de combat rassemblant des plateformes « habitées » et des plateformes automatisées, que sur des robots tout à fait autonomes. Au Pentagone, M. Brian Pierce a indiqué qu'un axe majeur du travail de la DARPA réside dans la « mise en équipe » de l'homme et de la machine – on parle de « *manned / unmanned teaming* » (MUM-T). En effet, selon les responsables d'IBM, la DARPA travaille surtout sur les technologies dites de « *combat mosaïque* », c'est-à-dire articulant tous types de plateformes, avec ou sans hommes, dans un système de combat « hybride ». La même logique sous-tend le programme d'études amont *Man–Machine Teaming* lancé par la DGA au printemps 2018 avec pour but d'intégrer des mécanismes d'intelligence artificielle à l'aviation de combat. Ainsi, **dans les « systèmes de systèmes » associant plateformes autonomes et plateformes habitées, des hommes demeurent au centre du dispositif**.

c. Le principe dit de « l'homme dans la boucle » doit demeurer au cœur de notre approche de l'automatisation des systèmes d'armes

Aux yeux des rapporteurs, et conformément aux principes de la doctrine française actuelle, il n'est pas envisageable que dans la décision d'engagement du feu, l'homme ne soit pas « dans la boucle ».

Les raisons de ce choix sont, bien entendu, avant tout d'ordre éthique. Aujourd'hui inacceptable socialement, le principe de « robots tueurs » ne paraît pas conciliable avec nos valeurs occidentales. Pour les rapporteurs, **c'est d'ailleurs la garantie du maintien de l'homme « dans la boucle » qui rend acceptables les recherches et les développements sur les applications de l'intelligence artificielle et de la robotique dans les armées**.

De surcroît, comme l'a fait observer le directeur du *Strategic Capabilites Office* du Pentagone, si l'intelligence artificielle tend à s'imposer dans les systèmes de commandement et de conduite des opérations comme la meilleure solution pour trier une masse considérable d'informations et limiter le besoin de transmissions, « ***l'intelligence artificielle, ce n'est pas de la magie*** ». En effet, les développements récents de l'intelligence artificielle ne permettent pas de penser avec certitude que les développements actuels permettront à court ou moyen terme de remplir deux conditions fondamentales :

– **doter l'intelligence artificielle de « *bon sens* », d'« *instinct* »**. En effet, les systèmes d'intelligence artificielle existants, comme ceux que l'on peut envisager à moyen terme, ne peuvent opérer que moyennant une phase d'apprentissage : tel est l'objet du *Machine Learning*. Mais, par définition, cet apprentissage se fait sur la base de connaissances, c'est-à-dire de situations stratégiques ou tactiques auxquelles il existe des précédents ou, du moins, que l'on peut prévoir. Or, aux yeux de M. William Roper, la surprise devient de plus en plus fréquente sur le terrain ; l'intelligence artificielle risque donc de ne pas être fiable face aux situations qui n'ont pas été vécues ou imaginées précédemment ;

– l'exploitation de l'intelligence artificielle dans les systèmes de combat supposerait aussi **que l'intelligence artificielle soit en mesure d'expliquer et de justifier les résultats de ses calculs**, comme il a été dit.

d. La doctrine devra évoluer de façon conforme à nos valeurs

La place de l'homme dans le combat numérisé, s'appuyant sur la robotique et l'intelligence artificielle, constitue donc un objet de travail doctrinal dont on pourrait résumer ainsi la problématique : **l'homme doit rester « dans la boucle », mais à quelle place précisément ?**

Une proposition du rapport précité de notre collègue Cédric Villani a retenu l'attention des rapporteurs car de nature à dépassionner ces débats et à préserver ces réflexions des écueils de la simplification : **établir une échelle définissant des niveaux bien identifiés d'autonomie d'un système d'arme**. Pour M. Cédric Villani, « *déterminer des échelles de l'autonomie : mines antipersonnel, systèmes téléopérés et automatiques, systèmes de défense antimissile, etc. […] permettrait de mieux identifier les technologies sur lesquelles l'on souhaiterait agir en excluant de la réflexion celles qui ne sont pas concernées par l'émergence de l'intelligence artificielle (les mines antipersonnel, notamment, souvent prises en contre-exemple) ou celles qui relèvent de la seule automatisation pour un besoin de performance* ». Ce rapport fait valoir que sur une telle échelle, « *des systèmes téléopérés, pilotés à distance, des systèmes de défense antimissile, torpilles, des systèmes de navigation et de guidage et les systèmes de surveillance et de détection ne sauraient être considérés comme des systèmes d'armes létaux autonomes* ».

La France a d'ores et déjà pris plusieurs initiatives au sein de la communauté internationale en vue de préciser les modalités d'application aux systèmes d'armes létaux autonomes au droit international de l'article 36 du Protocole I additionnel aux Conventions de Genève, qui vise à restreindre l'emploi de certaines armes nouvelles, au même titre que différentes armes conventionnelles dont ce traité limite l'usage. De façon cohérente avec l'impératif éthique consistant à ne pas risquer de placer nos soldats démunis face à des systèmes d'armes que la France se serait interdit de posséder pour des raisons éthiques, l'encadrement des systèmes d'armes létaux autonomes mérite d'être international. La poursuite des efforts de la France en faveur de l'élaboration d'une régulation internationale équilibrée mérite d'être encouragée.

C. LA TRANSFORMATION NUMÉRIQUE PERMET DES GAINS DE PRODUCTIVITÉ EN MATIÈRE « ORGANIQUE » SI LES ORGANISATIONS S'Y ADAPTENT

Non seulement les ruptures à venir dans les technologies numériques peuvent améliorer la performance de nos armes, mais elles peuvent accroître également l'efficience « organique » des armées.

1. La digitalisation des soutiens peut accroître leur efficience

Comme l'a reconnu M. Paul Serre, les économies permises par la transformation numérique sont souvent difficiles à quantifier. Une « méthode d'analyse et de remontée de la valeur », appelée MAREVA et conçue à l'échelon interministériel pour analyser l'intérêt financier des projets de système d'information, est systématiquement appliquée aux chantiers de numérisation. Elle prévoit une évaluation des coûts et des gains d'efficience, sous réserve de bonne fin de la conduite du projet. Dans la plupart des cas, l'exploitation des possibilités offertes par les technologies numériques paraît pouvoir créer des gains d'efficience substantiels. Parallèlement, les armées ont lancé des expérimentations de transformation digitale de diverses fonctions, relevant notamment du MCO des matériels et de la formation ou de l'entraînement des personnels.

a. La numérisation des procédures peut accroître l'efficience du maintien en condition opérationnelle des équipements

i. Enseignements tirés d'expérimentations de terrain

Au 12e régiment de cuirassiers, les rapporteurs se sont fait présenter les conditions et les premiers résultats de plusieurs des huit expérimentations qui y sont conduites par l'armée de terre. L'encadré ci-après présente l'un de ces chantiers dits « éclaireurs » qui consiste, au moyen de puces, à numériser le carnet de bord des véhicules, produisant des données précises pour chaque pièce de chaque véhicule, ce qui ouvre la voie à une optimisation de leur maintenance.

Expérimentation de moyens numériques de suivi des véhicules au 12e régiment de cuirassiers

Projets « éclaireurs » particulièrement structurants pour un régiment de cavalerie, un **carnet de bord digital** et un outil de **dématérialisation de la gestion des matériels d'une unité élémentaire** (DM@T) étaient en cours d'expérimentation au 12e régiment de cuirassier à la date du déplacement des rapporteurs.

Le carnet de bord digital doit permettre de remplacer le carnet de bord en papier, qui suit encore des standards de la fin des années 1940, ainsi que de faciliter le relevé des kilométrages et des heures d'utilisation en vue d'assurer un meilleur suivi de la disponibilité des véhicules et une meilleure programmation de leurs visites techniques. Il recense les utilisateurs de chaque véhicule ainsi que les activités pour lesquelles celui-ci a été utilisé.

Quant à l'application DM@T, conçue avec la structure intégrée du maintien en condition opérationnelle des matériels terrestres (SIMMT), elle doit rendre plus efficace la gestion des parcs de véhicules en facilitant la tenue à jour de leur inventaire et en simplifiant les démarches de perception des matériels dans les unités. Selon les explications de l'adjudant-chef responsable des matériels, il s'agit de simplifier une gestion des stocks qui n'est effectuée jusqu'à présent, au mieux, que sur Excel.

Les rapporteurs se sont fait présenter l'ensemble des matériels numériques servant à ces applications : instruments de saisie, ordinateurs reliés aux systèmes d'information de la maintenance, lecteurs de puces, *pad* de signature électronique, et divers modèles de puces. De plus, un dispositif portable, à peine plus épais qu'un *smartphone*, permet de lire les puces RFID placées sur les véhicules. Par rapport au système de saisie manuelle des données relevées tous les mois sur les 143 véhicules du régiment, en vigueur jusqu'alors, ce dispositif fait gagner une demi-journée et évite les erreurs de ressaisie. Un dispositif de télé-relève des données relatives aux véhicules serait certes plus performant encore, mais il suppose que les véhicules soient équipés de capteurs. Tel sera le cas pour les matériels de la gamme SCORPION, mais les équipements actuels ne sont pas tous pourvus de composants électroniques – l'adjudant-chef a cité le cas des camions GBC.

Une tablette permet en outre d'inscrire des données sur des puces vierges et de tenir les registres de perception de tous types de matériels. Elle remplace ainsi les livrets en papier de perception des matériels, facilitant la tenue des inventaires.

ii. La place de la numérisation dans la refonte de la chaîne de MCO aéronautique

La numérisation des procédures constitue l'un des leviers de performance au service de **l'ambitieux plan de refonte du MCO aéronautique** annoncé par la ministre des Armées.

En effet, comme l'ont indiqué les représentants du Comité Richelieu, la numérisation des données et la fiabilisation de leurs transferts sous-tendent la mise en œuvre du **mouvement de « verticalisation » contractuelle** désigné par la ministre comme une voie d'amélioration significative du MCO aéronautique. Cette réforme se traduira par un transfert à un nombre resserré d'industriels de stocks, de responsabilités logistiques et de maîtrise d'œuvre globale, sur le mode de ce qui a été conclu avec Dassault pour le système appelé « Rafale care ». M. Éric Trappier a d'ailleurs souligné qu'à l'export, une numérisation des

procédures de soutien plus poussée qu'en France garantit des taux de disponibilité élevés – même nettement plus élevés qu'en France.

Dans ce cadre, la digitalisation des procédures permet aux responsables des soutiens dans les armées d'exploiter au mieux les informations disponibles et de disposer des informations pertinentes pour la maintenance des matériels. Le Comité Richelieu souligne d'ailleurs que même dans un système de MCO en partie externalisé, les armées restent ainsi maîtresses de leurs données.

b. La numérisation des procédures peut faciliter la formation et la préparation opérationnelle des personnels

i. Le recours déjà ancien à la simulation et les développements de celle-ci

Le recours à des moyens numériques dans la préparation opérationnelle des militaires se traduit depuis de nombreuses années déjà par le **développement de moyens de simulation**.

Comme l'a expliqué la commissaire générale Françoise Latour, l'enjeu de la numérisation de la préparation opérationnelle est de « *réaliser un entraînement de niveau suffisant en limitant les coûts et l'usure sur les matériels opérationnels, tout en conservant un juste équilibre entre l'entraînement réel et virtuel* ». Cela suppose que les forces disposent de simulateurs représentatifs des équipements en dotation et, ce, en quantité suffisante, « *par l'interconnexion et la combinaison des outils de simulation pour augmenter le réalisme et pouvoir représenter les missions les plus complexes* ». Cela suppose aussi d'explorer *« des domaines émergents* », parmi lesquels l'état-major de l'armée de l'air cite le *big data*, l'intelligence artificielle, les *serious games* – c'est-à-dire les technologies de jeu appliquées à la formation – et la réalité virtuelle, pour étendre les possibilités de la simulation, « *par la prise en compte de nouveaux métiers ou le développement du niveau de réalisme ou de complexité* ».

Les rapporteurs ont pu observer le fonctionnement des moyens de simulation tactique d'opérations à bord des véhicules du 12e régiment de cuirassiers. Ils se félicitent aussi que le projet de loi de programmation militaire pourvoie au renouvellement de plusieurs équipements de simulation, et que nombre de programmes – à l'instar de l'opération SCORPION – comportent des dispositifs de **simulation « embarquée »**, c'est-à-dire à bord des véhicules.

ii. Des expérimentations tendant à numériser les procédures de suivi de la préparation opérationnelle

Certaines expérimentations visent à exploiter des gisements d'efficience dans la formation et la préparation opérationnelle des militaires. Ainsi, par exemple, les rapporteurs se sont fait présenter un projet dit « éclaireur » lors de leur déplacement au 12e régiment de cuirassiers : un « **système d'aide à une instruction de qualité** » (SAIQ) des personnels engagés dans l'opération Sentinelle. Cet outil vise à suivre, étape par étape, l'instruction des personnels en

vue de l'opération Sentinelle, et son expérimentation pourrait servir à préparer d'autres SAIQ pour d'autres types de missions. Il permet ainsi de formaliser un parcours de mise en condition avant l'engagement en opération, de capitaliser les contenus de préparation existants, de renouveler les supports d'instruction et d'évaluer le niveau des unités. Développé par un prestataire externe sur la base d'une « communauté *SharePoint* », cet outil coûte moins de 100 000 euros. Il permet une certaine standardisation de la préparation opérationnelle, son paramétrage ayant aussi pour enjeu d'éviter une centralisation excessive de cette activité, pour ne pas déresponsabiliser les « chefs de contact ».

Le 12e régiment de cuirassiers expérimente aussi un « **livret d'instruction virtuel élargi** » (LIVE), que présente l'encadré ci-après. Le colonel Olivier Kempf a fait valoir que ce projet est **emblématique d'une « logique d'urbanisation décentralisée » des systèmes d'information**, en ce qu'il devra être connecté à différents systèmes d'information, comme celui qui centralise les livrets de tir. Le dispositif devrait être livré avant l'exécution du plan annuel de mutations de 2018 pour une expérimentation « grandeur nature » fin 2018.

Le livret d'instruction virtuel élargi

Le projet de livret d'instruction virtuel élargi vise à dématérialiser à la fois le livret d'instruction de chaque militaire et les tableaux de bord interactifs de suivi des indicateurs de préparation de chaque escadron. Le logiciel développé à cette fin a pour objet de devenir l'outil unique de gestion des personnels et du quotidien dont dispose le chef de peloton. Il est pour l'heure testé sur Intradef, et pourrait être mis en place sur des tablettes. Ce livret virtuel a été développé par un lieutenant du 2e régiment de hussards, avec le soutien de la mission « innovation participative » de la DGA.

Selon les explications des chefs de peloton rencontrés par les rapporteurs, l'intérêt de cet outil tient à ce qu'il ne sert pas seulement à la **gestion des ressources humaines** – il est pour cela connecté au système d'information des ressources humaines de l'armée de terre Concerto –, mais aussi au **suivi individuel d'activité de chaque personnel**. À leurs yeux, il répond en cela à un besoin qui va croissant avec la **tendance au « panachage »** des unités : lorsqu'un chef de peloton se voit confier le commandement d'un groupe de circonstance, formé de personnels provenant de différents pelotons, il lui faut se faire rapidement une idée des capacités de ses nouveaux subordonnés.

D'après les démonstrations faites aux rapporteurs, cet outil permet en effet de recenser toutes les coordonnées des intéressés, diverses informations administratives – comme leurs numéros de passeports, que les chefs de pelotons mettent aujourd'hui un temps important à collecter en urgence avant les engagements en OPEX –, l'ensemble des activités accomplies par le militaire depuis le début de son service, ses performances en sport et au tir, ou ses qualifications diverses – du tir de toutes catégories d'armes aux permis de conduire –, ses états de service, ses habilitations, et jusqu'à ses mensurations pour l'habillement et l'équipement.

À ce stade du développement du livret virtuel, les cadres du 12e régiment de cuirassiers ont émis un avis très positif sur cet outil, « *très utile au quotidien* ». Ils ont fait valoir aussi que leur expérimentation avait permis d'identifier des champs souhaitables de développements supplémentaires de l'outil pour :

– assurer une **« remontée » automatique des informations** saisies dans le livret vers les applications pertinentes de l'intranet du ministère des Armées et les différents systèmes d'information « métier » de l'armée de terre ;

– rendre possible l'interconnexion du livret avec toutes sortes d'**objets connectés**, comme les capteurs RFID qui sont appelés à équiper un nombre croissant de matériels.

Le régiment expérimente également un **livret de tir dématérialisé** sur une tablette SMOBI. Il s'agit d'une application reprenant l'ensemble des règles et des compétences édictées par l'instruction sur le tir de combat (ISTC) et la base de données des personnels. Cette application permet au chef de groupe d'accéder à tout l'historique des performances au tir de ses hommes, de programmer leurs séances de tir et de les placer sur le pas de tir. Le premier bilan de l'expérimentation fait apparaître que l'application permet de **gagner quatre heures de tâches administratives** par séance de tir en groupe de vingt hommes. En effet, actuellement, les résultats de ces séances sont relevés manuellement, puis saisies dans un ordinateur par le chef de groupe, envoyés pour validation au bureau des sports, puis recopiés sur les feuilles individuelles d'instruction, avant d'être recopiés une nouvelle fois dans chaque livret individuel de tir. Cette procédure, où les recopies et les saisies manuelles sont nombreuses, est aussi fastidieuse que susceptible de comporter des saisies de données erronées.

Le colonel Olivier Kempf a expliqué que c'est par souci de méthode, suivant une **logique prudente de « petits pas »**, qu'il n'a pas été choisi d'essayer d'emblée de connecter le livret de tir aux systèmes d'information des armureries – pour accélérer les procédures de perception des armes et des munitions –, au système LIVE ou au SIRH Concerto. Néanmoins, le développement de l'application a prévu les **interfaces nécessaires, *via* des API**. Il a également souligné l'intérêt d'une architecture basée sur l'ISTC, jugeant de bonne méthode que **l'homogénéisation des pratiques précède le développement de solutions numériques**, car c'est souvent à l'occasion de la transformation digitale que se révèlent des failles dans la standardisation des usages et des procédures – on ne peut s'empêcher de penser à Louvois.

2. La transformation numérique des armées peut induire une profonde transformation de leurs organisations

Le général Bruno Maurice a souligné l'ampleur des changements qu'induit la transformation digitale des armées, citant le général américain Stanley McChrystal qui, dans son ouvrage *Team of Teams* (1), montre combien d'éléments « disruptifs » comporte la digitalisation pour les grandes organisations, « *notamment en ce que la "*shared consciousness*"* » – concept désignant l'appropriation des enjeux et des raisons de l'action par l'ensemble de ceux qui y participent – « *va de pair avec l'"*empowered execution*"* » – concept qui renvoie à l'idée de décentralisation des décisions concernant les mesures d'exécution.

(1) Général (R) Stanley MacChrystal « Team of Teams, New Rules of Engagement for a Complex World », éditions du New York Times.

Le rapport annexé au projet de loi de programmation militaire pour les années 2019 à 2025 reprend d'ailleurs cette logique, en indiquant qu'« *au-delà de l'adoption de nouvelles technologies, la transformation numérique est une démarche volontaire visant à* ***s'approprier au plus vite et dans les meilleures conditions les technologies émergentes, pour générer des évolutions significatives dans les usages et les modes de travail****, permettant* in fine *de mieux remplir les missions dévolues au ministère* ». Il s'agit ainsi de « *transformer les organisations et les domaines d'emploi* », en particulier en exploitant les données.

a. L'impact général de la transformation digitale sur les modes de travail et les organisations

Le général Bruno Maurice a constaté que les armées françaises sont « *restées en retrait dans la captation des innovations et des usages en matière organique* ». À ses yeux, les raisons en sont multiples ; il évoque notamment une « *acculturation digitale du commandement insuffisante* », la réorganisation des soutiens et l'« *atomisation des chaînes de responsabilité* » qui en a résulté, des tensions sur les ressources humaines et techniques, ou encore une « *hypersensibilité en termes de sécurité des systèmes d'information* ».

Il a défini la « transformation digitale » comme « *la rencontre d'une rupture technologique avec de nouveaux usages* », rendus possibles par la maîtrise de la donnée et de son traitement. Pour être exploitées, les données doivent être normées et sécurisées. Il s'agit donc d'abord d'un processus « métier », visant à créer de la valeur pour ses bénéficiaires : « *l'usager est au centre de la dynamique* ». Aussi la transformation digitale des armées vise-t-elle à « *stimuler l'innovation au plus près des usages* ».

i. L'usager et « les usages » au cœur des réflexions

Plusieurs caractéristiques de la « révolution numérique » peuvent en effet modifier les rapports et les méthodes de travail et, *in fine*, les organisations elles-mêmes, redéfinies autour des usagers et de la façon dont ils utilisent leurs outils professionnels. Ainsi, M. Marc Darmon, directeur général adjoint de Thales, a décrit comme le « cœur » de la révolution numérique « ***une attention soutenue, accrue et peut-être nouvelle pour l'utilisateur final – le militaire –, et pas seulement pour le client – le ministère*** ».

Des éléments comme **l'ergonomie des systèmes** ou, surtout, les dispositifs de **recueil des idées** avancées par leurs utilisateurs prennent ainsi une importance croissante dans les développements actuels.

Plus largement, la transformation digitale vise à intégrer davantage les usagers – en l'espèce, les personnels du ministère des Armées – dans le fonctionnement du ministère, en développant des liens d'interaction avec eux. Tel est d'ailleurs l'un des objectifs de la transformation digitale des armées énoncés par le rapport annexé au projet de loi de programmation militaire précité, qui vise à « *améliorer la relation au citoyen et aux personnels ainsi que l'attractivité du*

ministère » et précise que celui-ci « ***fournira des services dont l'accès sera plus aisé*** », grâce à la transformation numérique, « *pour les usagers, les personnels et leur famille* ».

À titre d'exemple, le 12e régiment de cuirassiers a testé une « **messagerie instantanée du chef de section** ». Il s'agit d'une application de messagerie comparable aux plus connues sur ce marché – comme *WhatsApp* –, sécurisée et installé sur les terminaux téléphoniques privés des militaires. Selon les cadres du régiment, les personnels lui ont trouvé peu d'avantages par rapport à *WhatsApp*, qu'ils utilisaient déjà. Une telle expérimentation aura permis de mettre en exergue le fait que « l'usage » d'un tel service préexistait à sa prise en compte par l'institution ; en cela, si elle n'a pas débouché sur un développement concret, elle n'en est pas moins riche d'enseignements. On notera qu'une application du même type, développée par Thales – donc française et sécurisée – sous le nom de *Citadel* est en cours de test pour l'état-major de l'armée de terre et donne, selon le colonel Olivier Kempf, toute satisfaction à ce stade.

Dans le même ordre d'idées, l'armée de terre développe également un « portail régimentaire », c'est-à-dire une matrice de site internet adaptable à chaque régiment, susceptible non seulement de présenter des informations générales sur l'histoire, l'organisation ou l'activité du régiment, mais aussi de comporter des espaces privatifs personnels pour donner aux soldats et à leurs familles un accès aisé, sans passer par l'intranet, à diverses informations ou démarches les concernant. Il s'agit là, même sur un mode moins interactif, d'**étoffer les liens entre l'institution et ses personnels**. Le projet de « portail régimentaire » vise aussi à garantir un certain degré de standardisation des sites internet des régiments ainsi qu'un bon niveau de sécurité informatique.

On soulignera que la population des personnels du ministère des Armées présentant une moyenne d'âge peu élevée, l'un des enjeux de la transformation digitale des armées réside dans l'adoption de modes de communication et d'interaction qui correspondent aux pratiques sociales des *digital natives*.

ii. L'importance de la maîtrise des données

Développer un environnement de liens numériques avec ses usagers suppose d'exploiter au mieux les données que l'on détient. La maîtrise des données et de leur traitement représente ainsi une condition de la transformation digitale des armées.

Les rapporteurs ont pu étudier un exemple concret avec l'effort en ce sens de l'état-major de la marine, qui conduit un projet de transformation profonde de son fonctionnement et de la gestion de ses relations avec ses personnels : **D@tamar**, que présente l'encadré ci-après.

Le projet D@tamar

Comme l'a expliqué le capitaine de vaisseau Laurent Célérier, il s'agit d'un « **lac de données** » où seront mises à disposition les données relatives au **fonctionnement organique de la marine. L'accessibilité de ces données permettra le déploiement d'applications nouvelles**, en particulier dans le domaine de la gestion de l'information. Ce système devrait constituer un net progrès par rapport aux outils qui prévalent aujourd'hui – les emails et les documents Microsoft Office. D@tamar sera **adossé à au projet Défense plateforme et accessible *via* Intradef**, le principal réseau de travail du ministère. Le chef d'état-major de la marine réfléchit par ailleurs aux voies et moyens d'un accès à certaines applications non sensibles *via* internet directement.

Comme exemple d'application d'un tel outil de valorisation et d'exploitation des données, le capitaine de vaisseau Laurent Célérier a indiqué que lorsque le ministère des Armées pourvoit au financement de la construction de crèches pour ses personnels, se pose la question de savoir où les implanter pour répondre au plus grand nombre possible de demandes. L'outil D@tamar pourrait permettre de cartographier les lieux de résidence des marins chargés de famille susceptibles d'avoir recours à ce service. Autres exemples cités : l'identification des locuteurs de langues rares parmi les personnels de toutes les catégories de grades, ou le repérage rapide des personnels ayant participé à une opération de secours à la suite d'un cyclone afin qu'ils puissent faire bénéficier de leur expérience les personnels appelés à être engagé dans une mission de même nature dans la même zone géographique.

Le rapport précité de notre collègue Cédric Villani souligne d'ailleurs, à propos de l'intelligence artificielle, les transformations que suppose la circulation des données dans les organisations. Reconnaissant les « *difficultés techniques* » associées à l'intelligence artificielle, il souligne à ce propos que l'« *on tend cependant à* ***sous-estimer largement celles qui relèvent des dimensions organisationnelles, structurelles et culturelles*** ». En effet, au sein d'une même organisation, « *les difficultés relèvent tout autant de la* ***capacité de différents acteurs à communiquer entre eux*** » ; l'exemple qu'il en donne est précisément la « *gouvernance de la donnée* », qui « *nécessite de mettre d'accord les métiers, les ingénieurs, les chercheurs, les administrateurs* ». Notre collègue démontre bien ainsi que « ***l'intelligence artificielle heurte l'héritage historique des organisations*** ».

iii. L'exigence d'« agilité » des organisations dans ces efforts de transformation digitale

L'adaptation des organisations aux évolutions rapides et continues des technologies numériques constitue une condition *sine qua non* de leur efficacité, ce qui **suppose qu'elles gagnent en « agilité »** pour intégrer les innovations, notamment les « usages » qui émergent dans la vie civile.

C'est en ce sens que la commissaire générale Françoise Latour a remarqué que dans le « *monde de la révolution numérique* », « ***toute entité peut être remise en cause, dans ses différentes dimensions, par une transformation accélérée des modes d'interaction, des rapports de force, des organisations et des métiers*** *sous l'effet de nouveaux usages rendus possibles par les technologies de l'information* ».

L'adoption de certaines technologies, comme l'intelligence artificielle, peut supposer des transformations particulièrement profondes. Ainsi, notre collègue Cédric Villani constate que « *les acteurs traditionnels restent peu matures sur la question* » car, selon lui, « *avant de se transformer et de se saisir du sujet de l'intelligence artificielle, il faut commencer par dissiper les peurs qui lui sont associées* ». Il explique également que « ***les administrations ne sont pas structurées de façon à accueillir de l'intelligence artificielle****, celle-ci étant par nature transverse à leurs missions* », observant notamment :

– un « ***héritage historique*** », c'est-à-dire une culture et des modes de fonctionnement « *défavorables au développement de l'intelligence artificielle, en particulier pour ce qui relève des processus, des achats, des pratiques en matière de systèmes d'information, de l'exploitation, de l'acquisition et de l'ouverture des données* » ;

– « *un effet de silo* », tant par « *manque de réflexion transversale et prospective sur des usages futurs* » que, souvent, par « ***crainte de perdre la maîtrise sur ses données*** », ce qui « *limite grandement la circulation des données* ***(y compris en interne)*** » ;

– **l'absence de « plateformes » rassemblant les données d'intérêt** pour l'intelligence artificielle, les moyens de calcul pour les exploiter et les « piles logicielles » nécessaires au développement d'applications, ce qu'un dispositif comme celui du projet D@tamar peut contribuer à résoudre.

b. L'impact de la numérisation sur les rapports du ministère des Armées avec les industriels

Évoquant le chantier de réforme du MCO aéronautique, M. Éric Trappier a estimé que « *la complexité de cette transformation pour la Défense tient en partie à ce que la numérisation a pour effet une profonde révolution dans les organisations elles-mêmes* ». À cet égard, plusieurs industriels regrettent que **la DGA ne soit pas connectée aux plateformes industrielles**. Selon M. Éric Trappier, cette difficulté avait été prise en compte par la DGA et les efforts pour la pallier sont poursuivis. Une première connexion, expérimentale, a ainsi été prévue dans le cadre du programme de rénovation de l'Atlantique 2.

Cependant, cette démarche reste largement à approfondir au gré de la réforme annoncée de la DGA car, « ***sans capacité de travail collaboratif, la DGA se priverait de possibilités industrielles*** ». En la matière, pour le président du GIFAS, « *la révolution numérique reste à faire* ». L'exploitation des technologies industrielles modernes permettrait par exemple **de simuler le comportement des équipements**, dans des laboratoires technico-opérationnels de pointe.

À cet égard, il y a lieu de se féliciter de ce que le rapport annexé au projet de loi de programmation militaire 2019–2025 mette en avant, au titre de la modernisation des procédures d'acquisition d'armements, « *trois leviers clé de performance* », parmi lesquels :

– « *le travail collaboratif et le décloisonnement des acteurs (équipes et plateau projet) à tous les stades* » ;

– « *l'utilisation des outils numériques* », citant le *big data*, l'ingénierie systèmes, la simulation, l'intelligence artificielle.

Ce rapport annexé précise que cette réforme « *tirera parti des meilleures pratiques appliquées dans le domaine civil et chez nos partenaires internationaux* », et sera appliquée à tous les nouveaux programmes d'armement ainsi que, lorsque cela sera possible, aux programmes en cours.

3. La transformation digitale suppose de résorber au préalable la « fracture numérique » dans les armées

L'exploitation des possibilités offertes par le numérique dans le quotidien des armées suppose des infrastructures informatiques robustes, à l'image des standards en cours dans les entreprises civiles. Or ces infrastructures sont aujourd'hui très inégalement déployées au sein du ministère des Armées, faisant apparaître une véritable « fracture numérique ». Aussi, aux yeux des rapporteurs, des investissements – d'ailleurs limités – sont-ils nécessaires pour que les armées puissent tirer pleinement profit des initiatives existantes et répondre aux ambitions de transformation digitale qu'elles se sont données.

a. Les infrastructures informatiques des armées sont marquées par une « fracture numérique » qui freine leur transformation digitale

i. L'équipement en infrastructures numériques est très inégal

Les rapporteurs ont été marqués par le fait que, selon le général Bernard Barrera, **seul un tiers des militaires de l'armée de terre dispose d'une adresse Intradef d'email professionnel**, tandis que l'accès à un poste de travail informatique est difficile pour un tiers des mêmes militaires. Pourtant, le fait de disposer d'un courrier électronique est très largement répandu dans les usages professionnels actuels, et peut être vu comme le strict minimum de la numérisation d'un environnement de travail. C'est en ce sens que l'amiral Arnaud Coustillière a pu constater « *une nette **fracture numérique*** ».

La couverture des emprises militaires en réseau d'accès à internet sans fil est elle aussi très limitée. **Une très large partie des emprises métropolitaines n'est pas couverte par un réseau wifi**. Le général Bernard Barrera a précisé que le « plan famille » annoncé en 2017 par la ministre des Armées est censé répondre à cette **condition préalable à la numérisation** de l'armée de terre.

L'investissement en la matière n'est pourtant pas considérable. L'amiral Arnaud Coustillière a en effet expliqué que sur le territoire national, la desserte des emprises du ministère en accès à internet relève :

– pour une centaine de sites, d'un réseau très résilient, opéré par la DIRISI, qui repose sur de la fibre louée « noire » ;

– pour un millier de sites, d'un contrat VPN souscrit auprès de la société Orange, qui fournit des connexions à un certain débit à l'entrée du réseau d'infrastructures militaires (c'est-à-dire, schématiquement, à l'entrée des emprises), le câblage final au sein des emprises restant à faire.

Pour le général Barrera, la mise en réseau des sites de la seule armée de terre coûterait environ 10 millions d'euros par an – en dépenses de fonctionnement mais aussi en crédits d'investissement pour la modernisation de réseaux obsolètes, souvent en cuivre et ne couvrant pas l'intégralité des emprises. Or elle n'est financée qu'à hauteur de 20 % de ce besoin.

Selon les estimations de la DIRISI rapportées par l'amiral Arnaud Coustillière, **la mise à niveau des infrastructures informatiques de l'ensemble des emprises du ministère coûterait 50 millions d'euros par an en tout, les crédits actuels n'en couvrant que la moitié**.

C'est également pour des raisons de coût et de lourdeur administrative que **doter les militaires de terminaux informatiques de télécommunications individuels – des *smartphones* – n'est pas mise à l'ordre du jour**. Aujourd'hui, les personnels gradés, dont les fonctions justifient un accès mobile à l'intranet du ministère des Armées, sont équipés de *smartphones* SMOBI. Ces dispositifs, distribués à 3 000 personnels sur les 300 000 agents du ministère, sont destinés à fournir aux cadres dirigeants un accès à Intradef et la possibilité de passer des appels téléphoniques cryptés. Chaque dispositif coûte en moyenne 1 000 euros.

Selon le colonel Olivier Kempf, **l'idée de généraliser SMOBI a été étudiée et expérimentée, mais écartée**. En effet, tant que seul un tiers des personnels de l'armée de terre possède un accès à Intradef, la plus-value d'un dispositif si coûteux est trop faible. Une plus large distribution d'équipements SMOBI fait néanmoins l'objet d'un « projet éclaireur ». À ce titre, le 12e régiment de cuirassiers a perçu 100 téléphones et 25 tablettes SMOBI, en vue de tester les différents projets et applications en développement. Mais le premier bilan de cette expérimentation fait apparaître la **lourdeur administrative** du dispositif. En effet, selon le capitaine en charge de ce projet, la perception d'un équipement prend une heure voire deux au personnel concerné, et une heure de plus à l'antenne territoriale de la DIRISI. Si un plus large déploiement des appareils SMOBI était envisagé, il faudrait tenir compte de cette contrainte.

ii. L'héritage informatique du ministère se traduit par des difficultés d'« urbanisation » des systèmes d'information

L'amiral Arnaud Coustillière a estimé que l'une des limites des infrastructures numériques actuelles du ministère des Armées tient à la **difficulté d'articuler les « silos » informatiques des directions « métiers » avec les services transverses**. Tel est l'enjeu de **l'urbanisation des systèmes**

d'information. La future DGNUM a d'ailleurs pour mission de veiller à la cohérence de la méthode et de l'urbanisation.

L'état des infrastructures numériques du ministère des Armées explique que, même pour déployer un « portail régimentaire » assez simple dans le cadre du projet « éclaireur » susmentionné, les efforts de transformation digitale se heurtent à d'importantes difficultés :

– la **maîtrise de l'hébergement** n'est pas simple, car la DIRISI ne s'est pas avérée être en mesure d'héberger le site et ses applications ;

– l'équilibre ne semble pas encore trouvé, dans la gestion des systèmes d'information, entre les **exigences contradictoires de centralisation et de décentralisation**. En effet, selon les explications du colonel Olivier Kempf, les systèmes d'information doivent suivre des règles d'urbanisation qui remontent pour l'essentiel aux années 1990 et restent très centralisées. Conséquence de cette difficulté d'adaptation aux pratiques plus décentralisées qui sous-tendent la transformation digitale, les applications des régiments sont souvent hébergés dans le secteur privé dans des conditions qui gagneraient à être davantage réglées par une base réglementaire et doctrinale précise et adaptée aux ambitions actuelles de transformation digitale des armées ;

– le développement de tels portails suppose des **compétences peu répandues au sein d'un régiment**. Dans le cas du 12e régiment de cuirassiers, en dépit du renfort d'un réserviste un jour par semaine et du télétravail qu'il peut accomplir, le départ en OPEX de l'officier de communication a constitué un frein majeur à une conduite rapide du projet.

b. Vers un « socle informatique » permettant de gérer à la fois l'héritage numérique du ministère et des dispositifs innovants de transformation digitale des armées

Réduire la fracture numérique du ministère en vue de faciliter sa transformation numérique suppose des investissements dans des infrastructures informatiques. Si ces investissements ne représentent pas un volume financier considérable au regard des moyens du ministère que le projet de loi de programmation militaire 2019–2025 propose d'accroître, ils doivent être ordonnés de façon cohérente, pour tenir compte de l'héritage du ministère et exploiter les technologies les plus prometteuses, comme le *cloud computing*.

i. Un projet d'ensemble : « Défense plateforme »

Comme l'a dit l'amiral Arnaud Coustillière, le ministère des Armées vient de connaitre douze à dix-huit mois de foisonnement d'initiatives et d'idées, très dynamique et positif ; « *les idées sont là et les "intrapreneurs" aussi* » ; il faut désormais « *canaliser cette démarche et en tirer des développements concrets* ». Pour ce faire, l'amiral a expliqué qu'il est nécessaire de « ***moderniser le socle informatique du ministère*** », ce qui suppose d'articuler, d'une part, des **éléments**

d'agilité – une capacité à développer des systèmes d'information en quelques mois au plus proche des métiers – et une **base informatique courante efficace**, gérant l'héritage informatique du ministère des Armées.

Tel est l'objet du **projet-cadre « Défense plateforme »** confié à la DGNUM et composé de quatre ensembles de chantiers :

– **l'identité numérique**, qui vise à doter chaque agent du ministère des Armées d'un « *avatar numérique* » ;

– **l'ouverture des données**, qu'il faut pouvoir annoter avant de les rendre accessibles *via* des portails de mise à disposition ;

– un **hébergement sécurisé**, automatisé et solide ;

– des **passerelles d'échanges sécurisées avec internet**.

Il faut donc offrir à chaque soldat un accès à diverses applications à partir de son outil d'accès quotidien à internet, c'est-à-dire son *smartphone*, pour qu'il puisse accéder à divers services (comme par exemple l'habillement). Dans ce chantier, un des principaux défis consiste à organiser le transfert des données des systèmes d'information actuels aux nouvelles applications.

La direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), qui joue le rôle de direction interministérielle des systèmes d'information, développe diverses applications et briques technologiques pour tous les ministères. La DGSIC du ministère des Armées a pour missions de les intégrer. Il en va ainsi, par exemple, du projet *France Connect*, que la DGSIC décline en moyens d'identification numérique.

ii. Les prometteuses possibilités des infrastructures de *cloud computing*

Comme l'indique notre collègue Cédric Villani, « *le* cloud *consiste à avoir accès, éventuellement par réseaux interposés, à des ressources de calcul (réseaux, serveurs, stockage, applications et services) éventuellement distantes, de façon transparente et avec intervention minimale du fournisseur de services* ». Ce rapport souligne l'intérêt du recours au *cloud computing* pour exploiter au mieux les progrès des technologies numériques.

Les rapporteurs observent que le *cloud* tend d'ailleurs à s'imposer comme une infrastructure de stockage, de traitement et de partage de données adaptée à la transformation numérique d'organisations complexes comme le ministère des Armées. Les Américains semblent résolument engagés dans cette voie.

- *Un axe majeur de la transformation digitale du* Department of Defense *américain*

L'orientation générale de la politique d'infrastructures informatiques du *Department of Defense* est marquée par une **transition vers les services de *cloud***

computing. M. Edward Brindley, adjoint à la *Chief Information Officer* (CIO) du Pentagone, a déclaré que « ***le cloud est une voie d'avenir*** », précisant que les armées américaines en restreignent pour l'heure l'usage aux informations non-classifiées, sous réserve d'ailleurs les informations en question aient vocation à être partagées. Les services de la CIO s'emploient ainsi à « *fluidifier* » la communication entre trois types de *clouds* :

– ceux développés par le ministère, régis par certaines règles spécifiques ;

– ceux que le *Department of Defense* a acquis auprès de fournisseurs civils, régis par des règles différentes ;

– ceux qui sont propres aux prestataires de services du ministère (les *contractors*).

Dans le cadre de cette transition vers le *cloud computing*, la politique choisie par le *Department of Defense* consiste à **exploiter au maximum les moyens civils, sous réserve de la sécurité des données**. Les services de la CIO ont mis en place à cet effet une procédure de tests de « management *du risque* » conduits par des personnels du ministère, des systèmes de plus en plus automatisés, ainsi qu'à l'occasion par des *hackers* dits « de confiance ». Le rapport précité de notre collègue Cédric Villani plaide lui aussi en ce sens : le concept de « *datacenter-as-a-service* » permettrait à la fois « *d'avoir des infrastructures gérées par un spécialiste du domaine* », et de « *faire monter en compétence* » cet opérateur dans d'autres développements technologiques, comme l'intelligence artificielle.

Bien entendu, un recours accru au *cloud computing* rend d'autant plus cruciale la **cybersécurité** des systèmes d'information. Ainsi, à titre d'exemple, les cadres d'*Amazon Web Services* ont précisé que leurs personnels exécutant le contrat de C2S susmentionné pour le compte des agences américaines de renseignement sont tous des citoyens américains disposant du niveau approprié d'habilitation, et la société propose d'appliquer les mêmes règles pour la mise en œuvre de tout autre contrat avec le *Department of Defense*.

Elles font valoir, surtout, que même dans les *data centers* classiques, il a pu y avoir des fuites de données, mais qu'avec les systèmes de *cloud*, la détection, l'attribution et la réparation des fuites est plus rapide, notamment lorsqu'elle repose sur des systèmes d'intelligence artificielle. En outre, le retour d'expérience du traitement des cas non conformes bénéficie à l'ensemble des agences partageant un même fournisseur de *cloud*. La sécurisation d'un *cloud* repose en outre, selon *Amazon*, sur l'idée de « **responsabilité partagée** » : l'opérateur garantit la sécurité de ses infrastructures, mais c'est à son client qu'il revient de sécuriser ses données.

Les niveaux de classification de certaines informations nécessitent parfois des séparations dans l'architecture des systèmes de *cloud*, et pas seulement des pare-feu (*firewalls*) informatiques ; néanmoins, *Amazon Web Services* observe que

le Pentagone a de plus en plus confiance dans les dispositifs de « **séparation logique** » – plutôt que de « séparation physique » – dans ces architectures. De façon générale, les responsables d'*Amazon Web Services* plaident qu'« *il faut rompre avec l'idée que le* cloud *n'est pas sûr ; si l'industrie financière y a recours, c'est que cette technologie présente des garanties* ». Commencer par y intégrer des informations sensibles mais non qualifiées est une bonne méthode pour prouver la robustesse de cette technologie.

Le rapport précité de notre collègue Cédric Villani en vient à la même conclusion. Il souligne que « *contrairement à une réaction instinctive, s'en remettre à un fournisseur de* cloud *ne revient pas à renier sur le niveau de sécurité* ». Au contraire, il fait valoir que « *faire le choix du* cloud*, c'est s'en remettre à un fournisseur spécialisé qui sera par nature plus compétent que l'écrasante majorité des organisations, notamment en matière de sécurité* ». En effet, la mutualisation des capacités permet d'éviter « *l'écueil classiquement rencontré : monter des infrastructures de calcul propres et de faible envergure* », facteur d'« *inefficience financière, écologique, et fonctionnelle* ». Le recours à des services de *cloud* extérieurs permet d'exploiter des effets d'échelle et va de pair avec la professionnalisation de cette fonction. Pour ces raisons, il estime souhaitable que les organisations publiques s'en remettent « *autant que possible à des fournisseurs dont c'est le cœur de métier* ».

- *Des atouts français à exploiter*

En France, l'utilisation de systèmes de *cloud computing* pour des applications du champ « organique » a été entamée en 2014, avec la mise en place progressive par la DIRISI d'un « *cloud* défense » qui repose sur quelques centres de données répartis sur le territoire national pour rendre accessibles, à distance, des informations relatives notamment aux ressources humaines, à la logistique ou aux finances du ministère des Armées.

Le rapport précité de notre collègue Cédric Villani sur l'intelligence artificielle montre que pour aller plus loin dans ce sens, la France peut s'appuyer sur « *des acteurs européens dont c'est le cœur de métier* », dans un contexte où « *les géants de la discipline sont essentiellement américains et chinois* ». Il cite principalement l'entreprise française OVH, qui à ses yeux « *semble avoir la capacité de donner la réplique sur un marché international* ».

4. Reste à promouvoir une véritable « culture de la donnée »

En fin de compte, les rapporteurs observent que la transformation digitale des armées suppose non seulement des investissements ponctuels, mais aussi – et surtout – une évolution culturelle dans le rapport de l'institution avec les données. Cela n'est pas propre aux armées ; avec la « révolution numérique », les possibilités d'exploitation des données par de nouveaux usages – et donc la valeur des données – s'accroissent considérablement dans l'ensemble des organisations.

Il va de soi que les spécificités des armées justifient une approche très prudente dans l'ouverture des données. Cependant, au moins dans le champ de leur activité « organique », il semble que des marges de manœuvre existent dans l'exploitation des données.

i. Les données prennent une place croissante dans la performance des organisations

- *Le volume de données produites croît considérablement*

Le ministère des Armées est un « producteur de données » particulièrement important, d'une part parce qu'il représente une organisation de grande envergure, d'autre part parce qu'il présente la spécificité d'exploiter nombre de « capteurs » d'informations.

Ainsi, à titre d'exemple, le système de transmissions tactique Auxylium produit à lui seul 1 To de données tous les mois. Selon le capitaine Jean-Baptiste Colas, qui en est l'initiateur et l'officier de programme, la DGA développe actuellement des outils d'intelligence artificielle pour exploiter ce *big data*, notamment à des fins de maintenance prédictive et d'anticipation des menaces.

- *Une exploitation efficace des données devient une condition de performance, tant opérationnelle qu'« organique »*

Pour reprendre l'expression des responsables de l'innovation chez Naval Group « *l'ère de la* data » est considérée comme marquant « *une quatrième révolution industrielle* » dans laquelle, notamment, le système de « jumeau numérique » des équipements ouvre de larges possibilités d'applications, y compris pour la maintenance, et constitue un facteur de compétitivité déterminant.

Une exploitation approfondie du potentiel des données conduira à devoir articuler trois « couches » de systèmes :

– une architecture ouverte et « *orientée vers les services* », constituant, dans l'exemple présent, l'infrastructure capacitaire de la force navale ;

– des données externes, à agréger de façon exhaustive au sein de l'infrastructure informatique embarquée pour leur traitement par des systèmes de *data management* ;

– des applications correspondant à différentes fonctions, comme par exemple les systèmes numérisés de maintenance, de lutte contre les menaces asymétriques, de lutte informatique (le *Cyber Management System*, appelé CyMS), ou de simulation embarquée pour l'exemple de la marine.

Dans chacune de ces « couches » comme dans leurs articulations interviennent également des dispositifs d'intelligence artificielle, des systèmes de « jumeau numérique » et diverses interfaces homme–machines.

ii. Le partage des données, nécessaire à l'innovation dans leur exploitation, constitue une lame de fond de l'économie numérique

Comme le souligne le rapport précité de notre collègue Cédric Villani sur l'intelligence artificielle, « ***en matière numérique, l'innovation repose bien souvent sur des logiques d'ouverture*** ». D'ailleurs, « *par nature, la donnée elle-même est propice à l'ouverture, au partage du fait de son caractère non rival et son faible coût de production* ».

La valeur des données – c'est-à-dire l'intérêt des usages que l'on peut en faire – tient rarement aux données elles-mêmes ; en effet, elles « *ont souvent peu de valeur, mais en gagnent quand elles sont contextualisées* », c'est-à-dire **croisées avec d'autres données**. Il est en effet fréquent que « *celui qui collecte la donnée ne soit pas le seul à pouvoir en tirer un bénéfice, ou le mieux placé pour l'exploiter* », d'où l'intérêt de favoriser leur circulation.

iii. La culture de la valorisation et du partage des données reste à promouvoir entre les différentes entités du ministère des Armées

Comme l'a constaté général Bruno Maurice, « *la culture du partage de la donnée reste à travailler* ». Si les usages civils prouvent l'intérêt du digital dans certaines fonctions organiques, la situation est inégale et la prise de conscience est parfois plus difficile encore en matière opérationnelle. Certaines unités sont très avancées – tel est le cas, par nature, de la direction du renseignement militaire ou des services compétents en matière de cyberdéfense. Mais « *pour d'autres, le potentiel du* big data *et de l'intelligence artificielle reste encore à démontrer dans le cadre de "hackathons" ou de défis* ».

À titre d'exemple, les rapporteurs relèvent que les données produites par les militaires utilisant le système Auxylium sur le territoire national ne sont pas partagées entre la force Sentinelle et les forces de sécurité intérieure, ce qui serait pourtant utile pour des informations d'intérêt tactique. Mais, selon le capitaine Jean-Baptiste Colas, « *le frein politique est tangible* », et « *va de pair avec un certain* ***protectionnisme des institutions concernant leurs données*** ».

Notre collègue Cédric Villani souligne lui aussi combien l'organisation « en silos » des systèmes de production et de stockage des données au sein de l'État peut constituer un frein à la circulation des données. Pour le cas spécifique des ministères des Armées et de l'Intérieur, il met en exergue deux freins supplémentaires :

– la **protection de l'information classifiée**, qui, à ses yeux, « *mérite une réflexion approfondie afin d'en simplifier l'appréhension à l'aune des nouvelles technologies* ». Il plaide en faveur d'une application raisonnée des règles de classification, voire de dispositifs de réduction du niveau de sensibilité de certaines données en vue de leur partage, « *par exemple lorsque la classification est issue des caractéristiques techniques des capteurs* ». Si une telle recommandation est bien entendu à prendre avec prudence, il n'en demeure pas

moins intéressant pour le ministère d'examiner la pertinence des pratiques actuelles de classification, au moins pour un partage de certaines données entre acteurs institutionnels. La refonte en cours du système de classification des informations pourrait en offrir l'occasion ;

– les règles actuelles de **sécurité des systèmes d'information**. Pour notre collègue Cédric Villani, sans remettre en cause la légitime exigence de sécurité des systèmes d'information, « *il faudra examiner certaines pratiques et déclinaisons* », de façon à « *repenser des contraintes de sécurité adaptées au contexte* » technologique actuel, notamment aux exploitations possibles par les technologies de *big data* et d'intelligence artificielle.

iv. La standardisation des données peut constituer un préalable utile à leur partage

Les représentants du Comité Richelieu, évoquant les gains d'efficience qu'une meilleure exploitation des données pourrait engendrer dans le système de MCO, ont regretté que **les données ne soient que peu standardisées**.

Dans le cas du MCO aéronautique, par exemple, un système d'information fourni par l'avionneur recueille les données techniques au pied de l'avion – souvent, aujourd'hui encore, par une clé USB – et il faut que les systèmes d'information logistiques des exploitants étatiques soient parfaitement compatibles avec ces données pour pouvoir en tirer tous les bénéfices. Or l'intérêt de certains industriels n'est peut-être pas toujours d'abandonner leurs propres formats de données au profit d'un format plus ouvert.

Dans ce cas, la nouvelle direction de la maintenance aéronautique pourrait gagner à une standardisation des données, non seulement pour améliorer la valeur ajoutée des services de MCO, mais aussi pour lui permettre de mieux suivre sa propre activité. D'ailleurs, pour les matériels terrestres, la structure intégrée de maintien en condition opérationnelle des matériels terrestres conduit un projet de digitalisation des échanges avec les industriels dont les résultats mériteront d'être suivis avec attention. De tels efforts de standardisation peuvent être vus comme d'utiles premiers pas dans l'appropriation d'une véritable « culture de la donnée ».

De surcroît, lorsque les données ne sont pas unifiées, standardisées et partagées en temps réel naissent des risques de ruptures de charge. C'est ce qui fait dire aux représentants du Comité Richelieu que « ***celui qui maîtrisera cette " continuité numérique de la donnée" pourra optimiser le soutien*** ».

D. LA TRANSFORMATION NUMÉRIQUE DOIT S'APPUYER SUR UN ÉCOSYSTÈME AGILE DE RECHERCHE, D'EXPÉRIMENTATION, DE DÉVELOPPEMENT ET D'ACQUISITION D'ARMEMENTS

Que ce soit pour exploiter des marges d'efficience dans des fonctions « organiques » ou pour conserver l'ascendant opérationnel de nos systèmes

d'armes, les armées, dans leurs efforts de transformation digitale, gagnent à s'appuyer sur un écosystème complet et diversifié de recherche, de R&D, d'expérimentation, de développements rapides et d'acquisition « agile ». En France, un tel écosystème reste aujourd'hui à consolider. Si les armées ne sont plus les principaux moteurs de l'innovation, elles ont néanmoins toute leur part à prendre dans le renforcement de cet écosystème.

1. Le ministère des Armées n'est plus le principal moteur de l'innovation numérique mais possède encore un rôle d'impulsion significatif

a. Dans la révolution numérique, la défense n'est plus le principal moteur de l'innovation

Alors que, dans la plupart des puissances occidentales dotées d'une industrie de défense forte, les innovations technologiques étaient souvent le fruit de programmes de recherche militaires, la situation semble partout s'inverser avec la révolution numérique.

Les rapporteurs ont d'ailleurs pu constater que les autorités civiles et militaires font le même constat même aux États-Unis, puissance pourtant réputée pour le dynamisme de son écosystème d'innovation militaro-industriel. Le colonel Paul Gillespie et le Pr. Steeve Bloor, professeurs à l'*Eisenhower School*, ont confirmé ce constat, qui résulte d'une inversion de tendance : même dans les technologies de l'information et de la communication, l'innovation était dans le passé le fait de la défense, mais elle est désormais le fait du secteur privé. Les représentantes d'*Amazon Web Services* ont confirmé cette analyse, déclarant que l'on ne peut plus voir le *Department of Defense* comme le principal moteur de l'innovation aux États-Unis : « *il conduit certes des études, produit encore certaines technologies "de niche"* », mais de façon générale, « *il trouve désormais intérêt à se fournir dans le privé* » pour ses équipements numériques.

Il ressort des travaux des rapporteurs que, ces dernières années, la DGA jugeait plus efficient de se concentrer sur l'intégration progressive des technologies numériques nouvelles développées par le secteur civil, plutôt que de soutenir un développement déjà (très) bien financé dans l'industrie civile. Selon la directrice de la stratégie de la DGA, **cette façon de s'en remettre au civil pour le développement des technologies a eu un effet pervers** : faute de levée des risques, l'intégration de systèmes civils est parfois plus compliquée qu'on ne l'avait imaginé. Les technologies du numérique sont dès lors autant de champs dans lesquels la DGA doit à ses yeux réinvestir.

b. L'État doit cependant conserver une politique industrielle volontaire dans des secteurs stratégiques comme la défense et le numérique

Outre l'intérêt qu'elles ont à suivre les développements des technologies civiles pour en lever les risques en vue d'un usage militaire, les armées et la DGA ont encore à jouer un rôle significatif d'impulsion, voire de planification.

i. En matière de numérique comme de défense, une politique industrielle volontaire est légitime et nécessaire

Comme l'a fait valoir le directeur général adjoint de Thales, des exemples récents montrent que dans le secteur de la défense, **la politique industrielle ne doit pas toujours reposer sur des mécanismes de mise en concurrence**. En effet, dans certains secteurs, des programmes d'études amont « *bien conçus* » ont été confiés à plusieurs industriels, successivement, représentant au total un niveau d'investissement important mais ne se traduisant pourtant par aucun programme concret. Tel est le cas par exemple pour les capacités d'écoute et d'interception des télécommunications : la France possède un grand industriel, Thales, quatre ou cinq PME ou branches de grands groupes très compétentes, et quelques compétences de pointe supplémentaires, par exemple chez Airbus. Ces différents acteurs ont été financés par des programmes d'études amont (PEA) relatifs à la guerre électronique de l'avant, sans aucune traduction capacitaire.

Comme le montre par ailleurs notre collègue Cédric Villani, une politique industrielle volontaire se justifierait pour des champs de développement numériques, comme l'intelligence artificielle. Pour les rapporteurs, une stratégie industrielle plus « colbertiste », s'inscrivant dans le respect des règles légales mais en exploitant toutes les marges de manœuvre possibles s'agissant de la défense, peut être plus pertinente que le libre jeu de la concurrence compte tenu, d'une part, des enjeux de souveraineté qui s'attachent aux technologies militaires dans un champ industriel dominé par les acteurs américains et chinois et, d'autre part, des moyens comptés du ministère des Armées.

ii. L'orientation de la R&D repose sur une vision prospective à long terme, qui gagnerait à être mieux partagée avec l'industrie française

Mme Frederick Douzet, titulaire de la chaire Castex de cyberstratégie de l'Institut des hautes études de la défense nationale (IHEDN), a souligné que – de façon peut-être paradoxale s'agissant de technologies qui font une large part à l'instantanéité et à l'« agilité » – **c'est bien une stratégie de long terme, suivie dans le temps long, qui est nécessaire pour prendre l'ascendant** dans un champ technologique. Elle a fait valoir que la Chine, par exemple, a élaboré une stratégie numérique très ambitieuse, notamment en matière d'intelligence artificielle.

Suivant la même logique, avec des moyens certes plus contraints, **la « révolution numérique » fait apparaître le manque d'une vision stratégique à long terme**, qui suive une ambition définie par l'autorité politique, soit déclinée par les armées et la DGA dans une démarche de prospective technico-opérationnelle et soit partagée avec les industriels partenaires du ministère.

- *Les études de prospective technico-opérationnelle ne s'inscrivent plus dans un cadre prospectif clair et global, guidé par un cap fixé par l'autorité politique*

Comme le dit M. Joseph Henrotin, chargé de recherches au Centre d'analyse et de prévision des risques internationaux (CAPRI) et à l'Institut de stratégie et des conflits (ISC), « *avec des moyens limités comme ceux de la France, l'agilité intellectuelle est nécessaire pour que l'innovation produise réellement de la liberté de manœuvre pour les forces* ». Ainsi, en matière de technologie, **un travail de doctrine est indispensable pour éviter d'éparpiller sans grand résultat des crédits comptés**.

Selon les explications de la directrice de la stratégie de la DGA, la vision de ce que seront les besoins des forces en armements dans trente ans fait l'objet de schémas directeurs partagés entre l'état-major des armées et la DGA. Cette vision était matérialisée par un « **plan prospectif à trente ans** » (PP30), qui n'est plus produit – l'ingénieure générale Caroline Laurent reconnaît que « *peut-être, d'ailleurs, est-ce un manque* ».

Son rôle est tenu aujourd'hui par **une trentaine de schémas directeurs** établis conjointement par la DGA et les armées, qui établissent les feuilles de route d'évolution des capacités jusqu'à un horizon de **quinze à vingt ans** : ainsi existent des schémas directeurs du combat sur terre, du combat aérien, de la sauvegarde maritime, etc. Il s'agit généralement de documents portant la mention « diffusion restreinte », qui peuvent faire l'objet de discussions avec les industriels. Ils se déclinent à plusieurs niveaux pour la programmation de divers crédits d'études. Cette trentaine de schémas ne forme toutefois pas un tout absolument cohérent car ils ne sont pas élaborés au même moment.

En parallèle, des organismes de réflexions et d'expérimentation existent. À Arcueil, la DGA possède un **centre d'analyse technico-opérationnelle de défense** (CATOD), qui associe des personnels de l'état-major des armées et de la DGA autour d'expérimentations. Le CATOD compte une centaine de personnels ; il a été développé pour les besoins de simulation des effets et des capteurs, et « *l'on peut le voir comme le centre de doctrine de long terme de la DGA* », comme le dit sa directrice de la stratégie. Les sujets d'études traitent ainsi diverses questions technologiques – par exemple : si l'on opère plutôt 100 petits satellites autonomes qu'un gros, quelles connectivités sont nécessaires ? Au sein des armées, le centre interarmées de concepts, de doctrine et d'expérimentations (CICDE) contribue aussi à ce travail prospectif. **Le rapprochement, voire la fusion du CATOD et du CICDE, fait l'objet de réflexions**.

Le général (2S) Jean-Marc Duquesne, délégué général du GICAT, a fait observer que jusque dans les années 2000, le collège des officiers de cohérence opérationnelle et architectes de systèmes de forces « *avait un rôle d'imagination, d'anticipation* » ; il a contribué à l'élaboration des concepts qui sous-tendent SCORPION. Mais rien de tel aujourd'hui ; l'état-major de l'armée de terre a cette

ambition avec « Action terrestre future », mais le produit de cette réflexion reste à ses yeux inspiré par les programmes actuels. Le renforcement d'un pôle d'expérimentation technico-opérationnelle et de doctrine autour du CICDE et du CATOD pourrait constituer un moyen de redynamiser l'émulation prospective parmi les responsables des programmes.

Il est à noter que le **centre de prospective et d'évaluation**, sorte de *think tank* placé auprès du ministre de la Défense à partir de 1964 qui se réunissait une fois par mois et fonctionnait de façon assez souple, a joué un rôle **d'« aiguillon » de la doctrine** en matière nucléaire d'abord, puis en matière informatique dans les années 1970, et enfin concernant le futur Rafale. Au fil des réformes successives, la DGRIS est aujourd'hui son héritière, mais aux yeux des observateurs, elle ne remplit pas la même fonction.

Parallèlement au rapprochement éventuel du CATOD et du CICDE, au niveau supérieur de la direction des efforts du ministère des Armées en matière de développements technologiques, **la recréation d'un organisme chargé, à l'instar du centre de prospective et d'évaluation, d'aider l'autorité politique à fixer des orientations de développement technologique à la DGA** pourrait permettre de redonner un cap de long terme à l'action de celle-ci. Un tel organisme serait le lieu le mieux désigné pour l'**élaboration d'un document global d'orientation stratégique tel que l'était le plan prospectif à trente ans**. Les représentants des trois groupements professionnels représentatifs des industriels de la défense ont d'ailleurs accueilli favorablement cette idée.

- *L'association des industriels à la prospective technico-opérationnelle de long terme mérite d'être renforcée*

La directrice de la stratégie de la DGA a expliqué que les industriels sont associés aux études technico-opérationnelles ; « *un temps, le ministère a voulu rester autosuffisant en la matière, mais de fait, il délègue largement ces études* ». Il est cependant difficile à la DGA d'y associer PME et *start-up*, qui ne dialoguent pas avec elle aussi étroitement que les grands groupes et qui peuvent difficilement travailler sur des études à large spectre technico-opérationnel.

Mais **l'association à tel ou tel programme d'études technico-opérationnelles ne suffit pas à donner un cap de long terme**, un cadre stratégique, aux partenaires industriels du ministère des Armées.

Ceux-ci conduisent eux aussi des travaux de prospective. Dans le cas de Naval Group par exemple, M. Éric Papin, directeur de l'innovation et de la maîtrise technique, a expliqué que la démarche d'innovation du groupe repose sur une approche prospective de long terme, à l'horizon 2040, d'où découlerait un « schéma directeur de la digitalisation et des concepts d'emploi », qui serait lui-même décliné en « modèles de répartition des fonctions » portant, par exemple, sur la place de l'homme dans les systèmes de combat naval, ou sur l'implantation à bord ou à terre de l'intelligence artificielle dans les systèmes de combat naval.

Dans cette démarche, Naval Group a proposé à la DGA de **formaliser cette stratégie par des « *feuilles de route "capacités / technologies"* » organisant des « *projets fédérateurs* »** qui visent à explorer l'articulation possible de capacités, de technologies et d'équipements innovants sur la base d'analyses partagées.

La **généralisation de ce type de « feuilles de route »** – ou de tout autre instrument du même type – serait de nature à associer les industriels à une démarche globale de prospective technico-opérationnelle.

L'investissement dans les technologies procède en effet de la préparation du futur, qui peut avoir tendance à passer à l'arrière-plan des priorités en période de tensions budgétaires. En conséquence, comme l'a constaté M. Éric Trappier, « ***c'est aujourd'hui par les programmes d'armement qu'est pilotée la préparation du futur, alors qu'il faudrait partir d'une logique inverse*** » : définir d'abord les conditions du combat futur pour, ensuite, en déduire les spécifications de programmes d'armement. Les représentants du GICAN ont fait valoir à cet égard que la modélisation du combat futur doit être vue comme de l'ingénierie de système appliquée au combat, et non aux matériels actuels.

M. Éric Trappier, rappelant que les industriels avaient commencé à développer des drones dès les années 1990 sans fervent soutien des armées, a rappelé que la **« pipeline »** de recherche et technologie (R&T) et de recherche et développement (R&D) **doit être alimentée très tôt dans le cycle de l'innovation**. Faute de quoi, la France en est contrainte à acquérir des équipements étrangers.

2. Détecter, stimuler, orienter et s'approprier l'innovation suppose d'animer un écosystème technologique agile

La plupart des observateurs s'accordent à considérer que la force des puissances qui ont le mieux su tirer parti de la « révolution numérique » au profit de leurs armées – les États-Unis et Israël – tient à l'existence d'un écosystème de R&D proche de la défense. Aux yeux des rapporteurs, des progrès sont possibles dans la structuration d'un écosystème français de technologies militaires.

Un tel écosystème est par nature un corps complexe. Il comprend un large champ d'activité, de la recherche amont – très éloignée des développements et des applications – à la R&D industrielle, l'acquisition d'un équipement et son appropriation – possiblement innovante – par ses usagers. Sa fluidité repose sur des relations de collaboration, des règles de fonctionnement et des procédures d'acquisition d'armement propres à favoriser les interactions entre l'ensemble de ses membres. Son agilité suppose aussi, bien entendu, qu'il soit irrigué par des flux financiers suffisants.

a. La stimulation d'un écosystème de recherche « tous azimuts »

La recherche est la source de l'innovation ; l'exemple bien connu des retombées de certains programmes de recherche financés par la DARPA suffit à s'en convaincre. Dans un contexte où la « révolution numérique » se traduit par

des convergences inédites entre plusieurs disciplines, notamment pour l'intelligence artificielle, consolider un écosystème technologique suppose non seulement de stimuler la recherche, mais d'ouvrir le champ de cet effort à un vaste éventail de disciplines.

i. Le caractère pluridisciplinaire de la recherche

M. Paul Théron, co-titulaire de la chaire « cyber-résilience Aérospatiale » (dite chaire « Cyb' Air ») de l'École de l'air, a insisté sur la **confusion qui est parfois faite entre recherche et innovation**. Le soutien aux *start-up* ou aux PME procède d'une logique de soutien à l'innovation – la définition de nouvelles solutions techniques –, mais ne peut pas sans abus être présenté comme un soutien à la recherche. Or « ***l'une ne remplace pas l'autre****, et si l'on néglige la recherche, à terme, on tarit innovation* ». Les rapporteurs ne peuvent que souscrire à ce constat.

Mme Frederick Douzet a d'ailleurs fait valoir que le soutien à la recherche est **trop souvent focalisé sur la recherche technique**. Pour elle, une ouverture aux sciences humaines et sociales est indispensable, ne serait-ce que pour la connaissance et l'anticipation de menaces de plus en plus complexes. M. Yvon Kermarrec, professeur à l'École nationale supérieure Mines-Télécom Atlantique et représentant la chaire « cyberdéfense des systèmes navals » de l'École navale, a ajouté que les aspects cognitifs, l'étude des réseaux sociaux, les aspects juridiques etc. des problèmes constituent un champ à exploiter dans la recherche, précisant que tel est l'intérêt des chaires : « *brasser différents profils autour d'une même finalité scientifique* ».

Dans un contexte de convergences entre champs disciplinaires autour de ruptures technologiques telles que l'intelligence artificielle, il importe en effet que le soutien à la recherche ait une **dimension véritablement interdisciplinaire**, ne se bornant pas aux sciences de l'ingénieur. Les rapporteurs soulignent d'ailleurs le caractère très interdisciplinaire des projets de recherches menés par l'agence qui fait figure de référence mondiale en la matière, la DARPA. Plus largement, les liens mériteraient d'être resserrés entre l'enseignement militaire supérieur et les différentes chaires spécialisées dans la défense, que présente l'encadré ci-après.

Les liens à resserrer entre l'enseignement militaire supérieur et les chaires pluridisciplinaires de recherche sur l'innovation dans le secteur de la défense

Les rapporteurs se sont attachés à s'entretenir avec les représentants des principales chaires françaises spécialisées dans le secteur des technologies de défense, non seulement pour alimenter leurs réflexions par le résultat de leurs travaux, mais aussi pour étudier la façon dont les armées peuvent tirer profit de cet écosystème de recherche pluridisciplinaire.

1. L'écosystème des chaires françaises spécialisées dans la défense

Ces chaires ont ainsi des structures de gouvernance **associant souvent les autorités militaires, des industriels et des chercheurs**. La chaire Cyb'air, par exemple, est dirigée par un comité directeur composé de représentants de l'état-major de l'armée de l'air et des groupes Dassault Aviation et Thales ; les bourses d'études sont attribuées après une sélection

de candidatures par un comité scientifique ; un troisième comité est chargé de la gestion quotidienne de la chaire.

● Les représentants des chaires à la table ronde organisées par les rapporteurs ont présenté leurs organismes.

M. Gérard de Boisboissel, secrétaire général de la chaire de cyberdéfense et de cybersécurité de Saint-Cyr, a présenté celle-ci comme plus spécialisée en sciences sociales et politiques – donc moins « scientifique » au sens strict – que les autres chaires. Elle travaille à des sujets tels que la conduite des opérations militaires, les changements induits par l'évolution technologique dans les organisations, ou les méthodes de gestion de crise. Autre particularité, cette chaire n'a pas de doctorants ; son budget se limite à 100 000 euros par an environ, ce qui lui permet de concentrer son activité sur l'organisation de journées d'études thématiques. Elle est hébergée par l'École spéciale militaire de Saint-Cyr à Coëtquidan, dont les élèves peuvent participer aux travaux de la chaire. Comme c'est toujours le cas pour les chaires placées auprès d'écoles, cette organisation a pour effet vertueux que les travaux de recherche de la chaire permettent d'irriguer l'enseignement.

Mme Frederick Douzet, titulaire de la chaire Castex de cyberstratégie de l'IHEDN, a expliqué que ladite chaire est hébergée par l'IHEDN et financée pour l'heure par le groupe Airbus. Ses travaux s'inscrivent dans le champ des sciences humaines et sociales et portent sur les enjeux géopolitiques et stratégiques liés au cyberespace. Sa valeur ajoutée réside dans ses efforts pour « *mettre en lien les sujets* » souvent abordés en silos. Un comité de pilotage de la chaire, associant tous les partenaires qui la soutiennent, décide du choix des sujets d'études, laissant une grande latitude aux chercheurs. Les relations avec le ministère des Armées sont à cet égard fructueuses. Avec 190 000 euros par an assurés pour trois ans, la chaire compte une titulaire, une chercheuse temps plein, un chargé de communication et un apprenti. Elle entretient des relations étroites avec l'Institut français de géopolitique de l'université Paris 8.

D'après M. Paul Théron, son co-titulaire, la chaire « cyber-résilience Aérospatiale » (dite chaire « Cyb' Air ») est le produit d'un partenariat entre, d'une part, des industriels qui la soutiennent (Dassault Aviation et Thales), y compris par conventions industrielles de formation par la recherche (CIFRE) et, d'autre part, l'armée de l'air, à travers sa fondation et son centre de recherche. Elle a noué divers partenariats, notamment avec des écoles doctorales et des laboratoires. Créée en juin 2017 et dotée de 170 000 euros par an, elle compte trois doctorants. Ses travaux portent principalement sur les « systèmes multi-agents de cyberdéfense ». M. Paul Théron a indiqué que la chaire entretenait des liens étroits avec les autres organismes de recherche de l'armée de l'air ou gravitant autour d'elle, précisant que la chaire et l'armée de l'air se mettent d'accord sur les axes de recherche, mais que l'armée de l'air ne les dicte pas – autrement dit, les thèses financées ne sont pas des projets informatiques « déguisés » de l'armée de l'air.

M. Axel Legay, directeur de la chaire « cybersécurité sur l'analyse de la menace » de l'INRIA a expliqué que cette chaire est soutenue par la région Bretagne et le pôle d'excellence cyber. Elle a identifié certains sujets de recherche comme étant stratégiques, parmi lesquels l'analyse des « *ransomwares* » et des « *malwares* ». C'est pour pousser les recherches en la matière que la chaire a été créée, en lien avec des industriels. Avec 500 000 euros de subvention de la région Bretagne, elle finance six thèses et six post-doctorats. Différents industriels (comme le Français Thales et l'Américain Cisco) ont noué des partenariats avec cette chaire – dont le budget est ainsi porté à deux millions d'euros – pour financer des recherches portant par exemple sur les « antivirus du futur », sur des algorithmes intelligents permettant d'exploiter des bases de données avec des technologies d'intelligence artificielle, ou sur des logiciels plus classiques, comme *Wannacry*.

M. Yvon Kermarrec, professeur à l'IMT Atlantique, représentant la chaire « cyberdéfense des systèmes navals » de l'École navale a indiqué que cette chaire a été instituée en 2014. Elle est soutenue par Naval Group et Thales, ainsi que par le conseil régional de Bretagne, *via* le « pôle d'excellence cyber », et entretien des partenariats étroits avec des acteurs académiques ainsi qu'avec la marine nationale. Elle emploie deux permanents, neuf chercheurs et plusieurs ingénieurs de recherche. Son programme de travail est établi pour trois ans par un accord entre les différents acteurs chaire – y compris la marine nationale – et porte aujourd'hui, pour une large part, sur les mécanismes de résilience. Cette chaire a également pour mission de contribuer à l'enseignement à l'École navale, par des actions d'enseignement et de sensibilisation ; d'ailleurs, certains élèves-officiers préparent une thèse au sein de la chaire.

● Les différentes chaires spécialisées dans les recherches sur la numérisation des armées semblent à la fois poursuivre des objets complémentaires, parfois spécifiques à une armée ou un milieu – évitant le piège de la redondance – et coopérer, ou du moins communiquer entre elles. Selon leurs représentants respectifs, la chaire de cyberdéfense et de cybersécurité de Saint-Cyr et la chaire Castex de cyberstratégie de l'IHEDN « *se parlent beaucoup*, via *les chercheurs* ».

2. Les liens entre les chaires et l'enseignement militaire supérieur

M. Patrick Hebrard a indiqué que l'enseignement et la recherche constituaient deux aspects indissociables de la mission de cette chaire, suivant un équilibre variable. Il a expliqué que l'accent sur la diffusion de la recherche avait pu s'imposer de façon particulièrement nette dans la marine du fait des spécificités de l'industrie navale. En effet, les navires modernes sont très « numérisés », et présentent donc un potentiel de vulnérabilité particulièrement fort, à prendre en compte, ce qui nécessite des travaux de recherche.

Selon M. Gérard de Boisboissel, **la soutenance d'une thèse par un officier-élève ou par un jeune officier n'est pas également valorisée dans toutes les armées** ; selon lui, l'armée de terre pourrait utilement favoriser la poursuite de doctorats par certains officiers, « *ne serait-ce que dans l'intérêt de sa représentation au sein d'instances internationales comme l'OTAN* ».

M. Yvon Kermarrec a précisé que même dans la marine, l'avenir d'un officier après son doctorat n'est pas nécessairement organisé de façon à exploiter au mieux ses compétences dans une optique d'« essaimage », de diffusion des résultats. Il a estimé cependant que les marins doctorants étaient de ce fait toujours volontaires, motivés par des sujets techniques souvent ambitieux et mobilisateurs. Mme Frederick Douzet a ajouté cependant que nombre d'élèves-officiers ou de jeunes officiers sont accueillis en master, notamment ès géopolitique.

ii. Soutenir la recherche très en amont

L'une des explications le plus souvent avancée à l'ascendant pris par l'industrie américaine dans la révolution numérique tient au soutien intense et continu dans le temps que le *Department of Defense* apporte à la recherche américaine *via* la DARPA.

Cette agence dispose en effet d'un budget annuel de l'ordre de trois milliards de dollars pour financer des projets de recherche à fort risque d'échec mais à fort potentiel en cas de succès, conduits très en amont du développement d'équipements ou d'applications. L'Agence a ainsi pour mission de préparer l'innovation de rupture. Parmi ses réussites passées les plus marquantes, on citera

le réseau ARPANET, ancêtre de l'Internet, l'ordinateur à interface graphique, ou encore le GPS. L'encadré ci-après présente le fonctionnement de l'Agence et l'orientation de ses travaux dans le domaine numérique.

La *Defense Advanced Research Projects Agency* (DARPA)

1./ Les missions et l'organisation de la DARPA

a) La mission historique de la DARPA : prémunir les forces armées contre toute « surprise technologique »

M. Brian Pierce, directeur du service de l'innovation dans l'information (*Information Innovation Office*) de la DARPA, a expliqué que la raison qui a conduit à la création de la DARPA en 1958 est la volonté de **garantir les forces armées contre toute surprise stratégique en matière de technologies**.

À ce titre, elle conduit des projets de recherche sur les **technologies de rupture** envisageables, dans un spectre très large d'applications possibles pour la sécurité nationale. En effet, la DARPA n'a pas pour mission de contribuer à la recherche en science pure, comme le fait la *National Science Foundation* (1) ; au contraire, la DARPA définit ses projets de recherche et les conduit systématiquement **dans l'optique de l'équipement des forces armées**, tant au niveau tactique que stratégique.

Pour autant, les projets de recherche ne sont pas définis en fonction de besoins précis, et encore moins de spécifications. En effet, de façon cohérente avec la mission de la DARPA, ses travaux ont un caractère prospectif et s'inscrivent **très en amont** des applications possibles : portant sur des technologies de rupture, il s'agit par nature de recherche « ***à haut risque d'échec*** », ce qui a pour corolaire des retombées très fructueuses en cas de succès. À titre d'exemple de cette **inscription dans le temps long**, M. Brian Pierce a cité le fait que la DARPA avait organisé son premier « défi » autour des véhicules autonomes il y a plus de dix ans.

b) L'organisation de la DARPA : un dispositif visant à garantir autant d'agilité et d'interdisciplinarité que possible

La DARPA est organisée en six services, compétents chacun dans un champ technologique : la biologie ; les sciences émergentes intéressant la défense ; l'innovation dans l'information ; la microélectronique ; les technologies d'intérêt stratégique (par exemple les technologies de renseignement, de réseaux, de C2 ou spatiales) ; les technologies d'intérêt tactique (c'est-à-dire principalement l'étude de nouveaux systèmes d'armes).

L'Agence compte **un millier d'agents, dont seulement 200 personnels civils ou militaires du *Department of Defense***, le reste de son personnel étant constitué de contractuels. Elle ne possède pas de laboratoire : elle confie la conduite de ses projets de R&D à des universités ou à des industriels, ce qui représente 90 % de son budget de trois milliards de dollars par an.

2./ L'orientation des travaux de la DARPA dans le domaine numérique

a) Une démarche « bottom-up *»*

D'après les explications de M. Brian Pierce, la DARPA n'a pas choisi d'établir une feuille de route très contraignante pour le choix de ses projets, car elle « ***préfère laisser venir à elle des compétences et des initiatives*** ».

(1) Fondation nationale pour les sciences.

● Tel est l'intérêt du mode de recrutement de la DARPA. M. Brian Pierce a expliqué que les responsables de programmes de recherche (*Program Managers*) **sont recrutés pour quatre à cinq ans seulement**, le brassage de personnels de différentes spécialités et leur renouvellement facilitant le brassage des idées et l'émergence de nouveaux sujets d'intérêt.

Ainsi, les personnels de la DARPA sont sollicités pour proposer des axes de recherche qui doivent répondre à trois critères :

– le caractère « *révolutionnaire* » de la capacité que peut conférer la technologie en question, par exemple les interfaces entre l'ordinateur et le cerveau ;

– une possibilité de rupture technologique, c'est-à-dire quelques éléments qui laissent penser que le projet n'est pas irréalisable à moyen terme ;

– un cadrage indicatif sur les délais et les coûts des recherches nécessaires, l'horizon de référence s'établissant autour de quatre à cinq ans.

● Pour la définition de ses programmes de recherche, la DARPA n'a pas recours à la procédure d'appel d'offres classique, mais à une procédure spécifique, dite de ***Broad Agency Announcement*** (1). L'Agence lance ainsi quarante à cinquante *Broad Agency Announcements* par an, qui permettent à différents laboratoires, aux États-Unis ou ailleurs, de mettre leurs idées scientifiques en compétition. La DARPA peut aussi recourir à des procédures moins publiques, selon le degré de sensibilité du projet concerné.

b) L'articulation de la DARPA avec la R&D privée

M. Brian Pierce a reconnu qu'avec la puissance de la R&D privée, notamment dans le domaine numérique, **le risque n'est pas nul de voir l'industrie privée « *doubler la DARPA* »** et le *Department of Defense* se fournir auprès de l'industrie privée.

● En règle générale, la DARPA essaie d'**éviter tout doublon** entre ses programmes de recherche et ceux de l'industrie privée. Ainsi, par exemple, elle a cessé de travailler sur les systèmes de traduction automatique devant l'avancée du secteur privé en la matière ; elle a borné ses programmes à l'apprentissage de langues rares.

● M. Brian Pierce a fait valoir, toutefois, que **les logiques sous-tendant la R&D privée et la R&D publique dans le domaine militaire ne sont pas strictement comparables**, notamment en matière de gestion du risque.

Par exemple, a-t-il expliqué, lorsqu'une société privée travaille sur les véhicules autonomes, tout l'enjeu pour elle consiste à réduire le risque de défaillance du système de pilotage au niveau minimal compatible avec les principes de l'assurance automobile. Les principaux développeurs civils de ces technologies ont pu tester leurs prototypes en les faisant rouler sur quatre millions de miles (4,6 millions de kilomètres), « *ce qui ne représente qu'un millionième de pourcent du nombre de kilomètres parcourus tous les ans par les véhicules réels* » ; aussi ces développeurs doivent-ils s'en remettre à des dispositifs de simulation pour compléter le *Machine Learning* de leurs systèmes de pilotage. Or de tels dispositifs de simulation sont eux-mêmes construits avec des marges d'erreurs basées sur des statistiques.

S'agissant en revanche de matériels militaires, qui doivent avoir une garantie de sécurité et d'efficacité maximale, M. Brian Pierce considère qu'il n'est pas possible d'apporter la preuve de leur bon fonctionnement sur la seule base de statistiques produites par simulation, c'est-à-dire au vu d'une **évaluation d'un risque simulé ramené à un niveau acceptable** dans une logique d'assurance.

(1) Avis public d'appel à idées.

En outre, M. Brian Pierce a estimé que si la recherche militaire et la recherche privée ont chacune leur place, **l'impératif d'efficacité opérationnelle des forces armées exige que la recherche militaire conserve une certaine avance technologique**, ne serait-ce que parce que les développements de la recherche privée sont plus rapidement disséminés dans le monde que ceux de la DARPA.

3./ Exemples de travaux de la DARPA dans le domaine numérique

M. Brian Pierce a présenté aux rapporteurs plusieurs travaux récents de la DARPA, parmi lesquels on citera par exemple un projet conçu pour améliorer le fonctionnement des prothèses posées aux soldats amputés, visant à développer des interfaces entre ces prothèses et le système nerveux – d'abord au niveau de la poitrine, puis au niveau du cerveau.

Si la DARPA vise toujours une application capacitaire pour ses programmes, il peut arriver que les armées n'en expriment pas le besoin dans l'immédiat. Tel est par exemple le cas d'une technologie acoustique de détection des départs de coups, mise au point par la DARPA dans les années 1990. L'armée de terre n'avait alors pas souhaité en disposer, jusqu'à ce qu'elle en éprouve le besoin pendant la deuxième guerre d'Irak.

Selon les indications de sa directrice de la stratégie, la DGA consacre actuellement 730 millions d'euros par an aux études amont, dont **85 millions d'euros « *en mode DARPA* »**, c'est-à-dire en « *financement sans retombées immédiates ou à finalité bien identifiée* ». Elle finance en outre 130 thèses. Même si le projet de loi de programmation militaire pour les années 2019 à 2025 propose d'augmenter le montant de l'enveloppe annuelle des crédits d'études amont pour la porter à un milliard d'euros, le volume financier consacré à la recherche « *en mode DARPA* » restera à l'évidence fort éloigné du budget annuel de cette agence.

Aussi la question de l'opportunité de créer, au sein du ministère des Armées, une sorte de « **DARPA à la française** » vient-elle régulièrement dans la discussion. Certes, il faut reconnaître avec le rapport précité de notre collègue Cédric Villani sur l'intelligence artificielle que le modèle de la DARPA est « *inspirant* ». Néanmoins, les rapporteurs en viennent à la même conclusion que lui : « ***chercher à répliquer ce modèle serait un non-sens*** », pour plusieurs raisons, tenant principalement au fait que l'on ne trouve pas de réel équivalent en France et en Europe de la force de frappe financière du Pentagone ainsi que du degré d'intégration du « complexe militaro-industriel ».

En revanche, dans la conduite de projets de recherche amont, **plusieurs aspects du travail de la DARPA pourraient justement inspirer la DGA dans l'allocation des crédits d'études amont** et l'utilisation des autres leviers de soutien à l'innovation, tels le financement de thèses et, dans une certaine mesure, les programmes d'investissements d'avenir :

– le recrutement de **directeurs de programmes indépendants**, experts ou chercheurs reconnus dans leur domaine, nommés pour une durée déterminée s'établissant généralement entre trois et cinq ans, ce qui confère à l'Agence son dynamisme et un haut niveau d'expertise ;

– un **haut degré de prise de risque**, quitte à ce que le taux de succès des projets ne dépasse pas 10 %, ce qui est assez éloigné des pratiques françaises ;

– des **cycles courts et dynamiques**, les programmes ne durant pas plus de cinq ans et pouvant être clos « sans drame » en cas d'échec prévisible, ou poursuivis par un autre programme dans une logique incrémentale, lorsque les résultats du premier sont prometteurs sans être immédiatement conclusifs ;

– **des objectifs précis d'usage, mais des spécifications technologiques qui ne sont pas prescriptives**, ce qui tend à garantir en cas de succès que le problème posé soit résolu tout en laissant aux chercheurs une grande souplesse dans l'innovation technologique ;

– un **financement suffisant**, concentré sur quelques équipes de chercheurs placées en situation de concurrence pendant une durée relativement courte.

Ainsi, s'il faut s'inspirer de l'exemple américain en matière de soutien à la R&D très en amont, **ce n'est pas en créant une nouvelle agence qu'il est le plus pertinent de le faire, mais plutôt en s'inspirant des méthodes de conduite de projet de la DARPA** dans la réforme annoncée de la DGA.

À cet égard, on relèvera que certes, la DGA finance des contrats de thèse, sur la base de sujets potentiels d'intérêt définis conjointement sur la base d'orientations énoncées par la DGA. Mais nombre d'observateurs s'accordent à juger que les demandes de la DGA ont souvent pour objet des innovations de nature plutôt incrémentale, certes de qualité, mais en réalité peu risquées. Il s'agit plus souvent d'améliorations de systèmes existants que de ruptures. Cela peut tenir à un biais culturel français : la crainte de l'échec, mère de l'aversion au risque.

Certains observateurs relèvent en outre que s'ils sont recrutés au plus haut niveau, les ingénieurs de la DGA suivent une carrière dont le prestige ne tient pas à des liens étroits avec les évolutions de la recherche tout au long de leur longue vie professionnelle. Aux yeux de certains chercheurs, « ***on ne peut guère être "observateur" de la recherche ; on doit la pratiquer*** ». Certains observateurs en concluent qu'une véritable rupture dans le fonctionnement actuel de l'écosystème de recherche et d'innovation dans le secteur de la défense consisterait à ce que certains ingénieurs recrutés par la DGA, lorsqu'ils sont conduits à piloter l'innovation de rupture, n'y fassent pas carrière à vie.

iii. Favoriser les liens entre l'industrie et la recherche

Ce n'est pas à l'État seul, bien entendu, qu'il revient de stimuler la recherche dans l'écosystème technologique de défense, même pour des travaux n'ayant pas d'application immédiate. Intensifier les liens entre l'industrie et la recherche est également nécessaire, et présente le double avantage de procurer au monde académique des moyens financiers supplémentaires et de faciliter la transition de la recherche à l'innovation.

Les efforts faits en ce sens par l'INRIA méritent d'être cités en exemple. L'INRIA dispose en effet de laboratoires communs avec des industriels, notamment étrangers ; l'expérience prouve, selon son directeur général, que la

coopération est paradoxalement **parfois plus facile avec les industriels étrangers** qu'avec les industriels français. En effet, les grands groupes étrangers prennent contact avec l'INRIA pour des projets sur lesquels ils ont travaillé de longue date ; par exemple, Samsung travaille à l'isolation de la voix humaine pour qu'un appareil électroménager puisse la distinguer des bruits alentours. Sollicitant l'INRIA avec un but précis, ces partenaires connaissent la valeur des travaux de l'Institut… et consentent à en payer le prix. Avec certains groupes français, les contacts sont pris à un très haut niveau hiérarchique, ce qui a pour corollaire un niveau tout aussi élevé de généralités dans les premières discussions et, dès lors, des difficultés pour en venir à des applications concrètes se traduisant par des coopérations dûment financées.

Cela tient au cloisonnement, pas encore totalement assoupli, entre la recherche et l'industrie en France ; cela tient aussi, pour partie, au statut public de l'INRIA, qui peut donner l'impression que le service de l'Institut est un dû. M. Antoine Petit et Mme Isabelle Ryl ont toutefois souligné qu'il ne fallait pas faire de ce constat une règle générale, citant entre autres EDF comme un partenaire avec lequel les coopérations sont poussées et mutuellement fructueuses.

L'intérêt de ces coopérations, pour les industriels, est d'**avoir accès aux chercheurs comptant parmi les meilleurs du monde pour préparer des innovations de rupture**. Contrairement à une société de services, l'INRIA n'a pas d'obligation de résultat ; ses chercheurs collaborent avec des industriels dans une logique d'obligation de moyens, ce qui est cohérent avec la part incompressible de risque accepté qui existe dans toute recherche d'innovation de rupture. Les questions de propriété intellectuelle se posent avec moins d'acuité qu'ailleurs car l'INRIA produit essentiellement des logiciels : d'une part, ceux-ci ne font pas l'objet de brevets en tant que tel et, d'autre part, la valeur d'un logiciel tient à ses concepteurs, capables de le faire évoluer, plutôt qu'à un état de leur programmation.

Ainsi, l'INRIA tire environ 60 millions d'euros par an de ses ressources propres, sur un budget annuel de 230 millions d'euros en moyenne ; la part de ressources propres tirées de coopérations avec le secteur privé représente 10 % environ des produits de l'Institut. Ces ratios sont assez stables, **le financement public permettant à l'INRIA de travailler sur des technologies de rupture n'ayant pas encore d'application**.

Surtout, **l'INRIA crée des *start-up***, à raison d'une dizaine par an, contre la moitié il y a quelques années. M. Antoine Petit a signalé que ces *start-up* sont régulièrement rachetées par des grands groupes étrangers, comme IBM ou Apple, notamment lorsqu'elles ont déjà un succès avéré et se trouvent entravées dans leurs ambitions de croissance faute de financements disponibles. Selon lui, cette difficulté tient à ce que si la création de *start-up* est correctement soutenue par les instruments financiers disponibles sur la place de Paris, tel est moins le cas de leur croissance. Mme Isabelle Ryl a cité en exemple le cas d'une *start-up* créée par des chercheurs du centre parisien de l'INRIA, qui avait développé un système de

classement d'images intégrant les goûts de l'utilisateur par des techniques dites de *deep learning* ; Apple a racheté la société et engagé ses fondateurs – qui en constituent la véritable valeur – et les a délocalisés en Californie.

Interrogés sur les pratiques ayant cours dans les autres pays pour tisser des liens entre les mondes de la recherche et de l'ingénierie, les dirigeants de l'INRIA ont cité en exemple le cas de M. Yann Le Cun, qui, tout en dirigeant le département d'intelligence artificielle de *Facebook*, est encore titulaire d'une chaire à la *New York University* – ainsi d'ailleurs qu'au Collège de France en 2016. D'autres exemples de même nature montrent une **grande porosité entre le monde industriel et le monde académique** dans les pays les plus puissants du point de vue de l'innovation technologique.

Ces exemples montrent l'intérêt qu'il y a à associer plus étroitement la recherche et l'industrie. Si les difficultés constatées ne concernent pas seulement le secteur de la défense, le poids particulier du ministère des Armées dans ce secteur industriel lui confère des leviers d'action particuliers pour structurer cet écosystème.

b. La détection des évolutions technologiques et les liens entre les armées et les entreprises innovantes

Dans l'appropriation de l'innovation technologique par les armées, l'un des enjeux tient à la détection des innovations. En effet, il apparaît que dans la « révolution numérique », l'innovation est moins souvent le fait des grands cocontractants habituels de la DGA que celui de *start-up* nées dans le secteur civil, que rien ne conduit à se tourner spontanément vers le ministère des Armées.

i. Le développement des « labs »

Cette situation suppose de créer des lieux de contacts entre *start-up* et armées, pour permettre à ces industriels de présenter aux forces des produits répondant à leurs besoins. Le ministère des Armées a consenti d'importants efforts en ce sens, particulièrement en direction des nouveaux industriels du secteur numérique, avec la **création d'organismes appelés « labs »**. Le premier et principal de ces « labs » est le « DGA Lab », que présente l'encadré ci-après.

Le « DGA Lab »

1./ Les objectifs et les méthodes du « DGA Lab »

Le « DGA Lab » a pour mission d'accélérer l'appropriation de l'innovation par le ministère des Armées. Une telle appropriation suppose de détecter et d'expérimenter les technologies prometteuses ; selon ses responsables, le « DGA Lab » est ainsi « *là où les militaires et la* French Tech *se rencontrent* ».

Cet organisme a été créé en 2013, quand la DGA a voulu créer un laboratoire visant à stimuler l'innovation dans le cadre du programme de système d'information des armées (SIA). Depuis lors, le « DGA Lab » a élargi son champ d'activité à l'ensemble des secteurs de la défense, les projets innovants restant essentiellement numériques, du fait de la nature de l'innovation aujourd'hui.

Le programme de travail du « DGA Lab » articule plusieurs types d'événements :

– une session thématique mensuelle, réunissant trois sociétés complémentaires (et non concurrentes, afin d'éviter des pertes de temps), visant à identifier les technologies répondant aux défis opérationnels. 35 à 40 représentants du ministère des Armées se voient présenter trois solutions, en 45 minutes, et en discutent dans un cadre plus ou moins informel. 44 sessions ont été tenues à ce jour ;

– depuis 2014, des petits-déjeuners sont souvent ouverts au secteur privé, voire aux « institutionnels », dans une démarche d'*open innovation*, c'est-à-dire avec présentation de technologies et RETEX opérationnels. 35 réunions se sont tenues depuis 2014 ;

– des activités *ad hoc*, avec des sessions particulières, pour la ministre, le DGA, les rapporteurs, ou, prochainement, le collège des inspecteurs généraux.

Il s'agit, selon les responsables du « DGA Lab », d'une « ***démarche itérative de co-innovation*** ». En effet, le dialogue au sein du « DGA Lab » a ceci d'itératif que les opérationnels imaginent de nouveaux usages.

Au total, les activités du « DGA Lab » ont réuni 3 000 participants, débouché sur 130 solutions proposées, avec 32 % de concrétisation. Pour les responsables du « DGA Lab », une chance sur trois de concrétisation représente déjà un taux de réussite intéressant.

2./ Les défis organisés par le « DGA Lab »

En plus d'organiser des rendez-vous réguliers entre « opérationnels » et *start-up* ou explorer les technologies nouvelles, **le « DGA Lab » a pour mission de concrétiser ces démarches par des « défis »**.

Le premier de ces défis a concerné l'équipement des forces spéciales en drones dits « *indoor* », c'est-à-dire capables de voler à l'intérieur de bâtiments. L'idée a été lancée en 2016, puis l'écosystème industriel a été sondé à l'occasion d'une réunion rassemblant une centaine de techniciens et d'utilisateurs en janvier 2017, et une procédure d'acquisition rapide a été mise en œuvre, découlant sur dialogue compétitif de dix mois. Conformément au code des marchés publics, les compétiteurs ne connaissent pas leurs concurrents. Pour les responsables du « DGA Lab », c'est là une limite du système. Ouvert à toutes propositions, ce dialogue compétitif a suscité douze candidatures sur dossiers, six étant retenues pour la fabrication de démonstrateurs. En 2018, le gagnant se verra attribuer un programme d'équipement par la DGA.

Compte tenu des besoins de capitaux des *start-up*, la procédure retenue prévoit **l'indemnisation des compétiteurs à chaque étape du dialogue compétitif**, avec 10 000 euros pour la remise d'un dossier de candidature, 25 000 euros pour ceux qui sont retenus, et 150 000 euros pour ceux qui auront présenté des démonstrateurs.

Dès lors qu'ils s'adressent à des *start-up*, ces défis doivent déboucher sur des programmes d'armement définis de façon un peu différente des contrats classiques passés avec les grands groupes industriels. En effet, s'agissant de fournisseurs nouveaux pour le ministère des Armées, **la DGA se doit de tester la fiabilité de leurs capacités industrielles**, c'est-à-dire leur aptitude à passer du stade du prototype ou de la démonstration à celui de l'industrialisation. C'est pourquoi les volumes commandés sont dans un premier temps limités ; dans le cas des drones « indoor », le marché porte sur quelques dizaines d'appareils, avec des bons de commande permettant, le cas échéant, de porter leur nombre à cent.

L'intérêt de ces défis réside aussi dans le fait d'accompagner les entrepreneurs dans le développement d'une offre qui pourra être proposée par la suite à d'autres usagers – par exemple les pompiers dans le cas des drones « *indoor* ». Les armées auront ainsi poussé les *start-up* à améliorer leur offre.

Dans une période très récente, plusieurs autres projets de « labs » ont vu le jour, à l'image du « N@vyLab » de la marine, du projet de « *Battle Lab* » de l'armée de terre, du « SGA Lab » du secrétariat général pour l'administration du ministère, ou de l'incubateur de *start-up* et du *Air warfare center* (le centre d'expertise aérienne militaire) de l'armée de l'air à Mont-de-Marsan.

Même des services de renseignement, dont l'activité ne se prête pas par nature à une large publicité, développent des projets de ce type. Tel est le cas notamment de l'*Intelligence Campus* que la direction du renseignement militaire propose de créer sur la base de Creil. Le général Jean-François Ferlet a expliqué que cette structure viserait avant tout à rapprocher les services de renseignement des *start-up* et autres industriels des services de renseignement. Ce projet poursuit trois finalités :

– resserrer les liens de la DRM avec le monde de la **recherche appliquée**, c'est-à-dire « *mettre en contact les utilisateurs avec les développeurs de solutions technologiques* », afin de **maintenir à jour les compétences technologiques des opérateurs** et leur connaissance de l'innovation ;

– rapprocher aussi la DRM du **monde académique** : l'*Intelligence Campus* est « *né de la prise de conscience de l'intérêt qu'a la DRM à se rapprocher du monde universitaire et académique* », intérêt d'autant plus clair qu'« ***orienter une thèse** permet un gain à faible coût* » ;

– servir d'« **incubateur d'idées** » : pour aller plus loin dans les développements concrets des idées innovantes, l'*Intelligence Campus* permet de développer des outils « *en boucle courte* », « *en mode agile* ». La DRM peut, à cette fin, mettre en œuvre des « **défis** », comme en mai 2017 pour la reconnaissance automatique de véhicules.

Outre qu'ils permettent des contacts directs entre les armées et des industriels qui ne font pas partie des fournisseurs habituels du ministère, ces démarches « en boucle courte » présentent aussi l'avantage de **faire aux « opérationnels » une plus large part que d'habitude dans les processus d'acquisition** d'armements. La forme du défi permet d'ailleurs d'éviter à l'acheteur public d'être trop prescriptif s'agissant des technologies susceptibles de répondre à ses besoins.

C'est en ce sens que le directeur général de l'INRIA a souligné que « *l'expression des besoins est une clé de la programmation* », regrettant que « *souvent, on mélange la question (comment servir tel ou tel usage ? faire telle ou telle chose concrète ?) et la réponse, c'est-à-dire le choix technologique* ». Pour lui, « ***sans les utilisateurs finaux, pas de travail fructueux*** ». Or « *la distance entre chercheurs et utilisateurs finaux est souvent grande, d'où **l'importance des "traducteurs", des interfaces*** » ; **pour lui, la DGA et les centres de R&D des industriels pourraient tenir ce rôle** davantage qu'ils ne le font parfois en France, « *à l'image de ce qui semble fonctionner plus aisément à l'étranger* ».

La recherche et la R&D gagneraient donc à des contacts plus étroits avec les utilisateurs des technologies. Par exemple, l'utilisateur d'une technologie robotique peut juger sans gravité qu'un robot bute dans 1 ou 2 % des cas dans un scénario de progression en milieu terrestre ; mais faute de liens avec les utilisateurs, les marges d'erreur retenues par les laboratoires de R&D peuvent être trop exigeantes, donc sous-optimales. L'étroitesse des liens et la qualité du dialogue entre les laboratoires de R&D ou la DGA, d'une part, et les utilisateurs des technologies fournies par la BITD française, d'autre part, méritent donc une attention approfondie.

ii. Les recommandations méthodologiques du rapport de notre collègue Cédric Villani sur l'intelligence artificielle

Le rapport précité de notre collègue Cédric Villani comporte une série de recommandations qui paraissent de nature à approfondir la démarche engagée avec la création des « labs » en vue d'adosser notre politique d'équipement de nos armées sur un écosystème technologique innovant. Il retient d'ailleurs le secteur de la sécurité et de la défense parmi quatre secteurs prioritaires pour une politique ambitieuse de soutien au développement de l'intelligence artificielle. Ses conclusions concernant cette technologie sont pour beaucoup d'entre elles applicables pour d'autres technologies numériques innovantes dans le secteur de la défense. Il formule notamment les propositions suivantes.

- *Mettre des **corpus de données** à disposition de viviers d'entreprises innovantes*

Il s'agit de permettre à ces entreprises de disposer de la « matière première » nécessaire à leurs développements numériques – c'est-à-dire des données en masse et, de préférence, annotées –, et créer ainsi de nouvelles technologies et de nouveaux usages de ces données.

Le rapport précité de notre collègue Cédric Villani souligne que la politique de gouvernance des données doit être « adaptée à chaque secteur ». Une telle recommandation est en effet à prendre avec prudence s'agissant de la défense, et ne peut concerner que des données non classifiées. Mais l'exemple mentionné plus loin du défi relatif à l'exploitation des images pour la surveillance maritime montre que même dans le champ de la défense, de tels corpus exploitables de données non classifiées existent.

- *Expérimenter des « **plateformes sectorielles** »*

On entend par « plateformes sectorielles » des **services assurant une fonction d'intermédiaire dans l'accès aux informations, aux contenus, aux services ou aux biens** édités ou fournis par des tiers. « *C'est un modèle de développement à l'efficacité redoutable, qui fait la force des géants chinois ou américains* ». De telles plateformes permettraient « *à des écosystèmes de se structurer autour des fonctionnalités qu'elle met à leur disposition* ». Concrètement, le rôle de ces plateformes consisterait par exemple à assurer la

captation ou la collecte de jeux de données utiles aux développements industriels, à déployer des interfaces applicatives de programmation pour favoriser les échanges entre les acteurs d'un même écosystème, à négocier la mise à disposition de capacités de calcul de pointe et à accompagner les entreprises innovantes dans des démarches d'expérimentation et d'accès aux marchés.

Il serait intéressant d'étudier la façon dont une telle fonction pourrait être remplie par **les « labs » ou par des organismes développés autour des « grands » industriels « plateformistes »**.

- *Organiser de grands **défis** articulés avec les enjeux sectoriels*

Notre collègue Cédric Villani déplore que « *le soutien à l'innovation sous forme de défis occupe aujourd'hui une place limitée dans l'approche publique du soutien à l'innovation* », alors que **cette méthode a prouvé son efficacité**, notamment aux États-Unis avec les défis lancés par la DARPA. Ceux-ci doivent afficher « *des objectifs clairs, quantitatifs et opérationnels et, malgré tout, suffisamment ambitieux pour stimuler la capacité d'innovation* » avec, à la clé, des « *récompenses financières importantes* ».

Cette recommandation est tout à fait conforme aux pratiques des « labs », qui méritent d'être intensifiées.

- *Mettre en place des **« bacs à sable » d'innovation***

Le rapport précité de notre collègue Cédric Villani plaide en faveur d'aménagements réglementaires et administratifs circonscrits, visant à faciliter les démarches expérimentales. Ce qu'il appelle des « bac à sable » d'innovation s'entend d'un triple aspect :

– un **allégement temporaire de « *certaines contraintes réglementaires* »** pour « *laisser le champ libre à l'innovation* », le rapport citant l'exemple de la réglementation de l'aviation civile pour les expérimentations d'essaims de drones ;

– un **accompagnement** administratif et réglementaire des acteurs ;

– des **moyens d'expérimentation en situation réelle**, c'est-à-dire des terrains d'expérimentation que, souvent, « *seule la puissance publique est en mesure d'offrir* » et qui constituent, pour les entreprises innovantes, à la fois « *un facteur d'attractivité majeur* » et « *un avantage singulier* » sur leurs concurrents. Compte tenu des spécificités des activités militaires et des équipements employés, les armées sont particulièrement concernées par cette proposition.

C'est au sein de tels « bacs à sable » constitués pour les besoins de la défense que notre collègue Cédric Villani recommande de :

– permettre l'accès des acteurs économiques à des « *données opérationnelles* » et, ce, « *dans un cadre maîtrisé* » par le ministère ;

– produire des « *jeux de données d'intérêt exportables* » sur différents cas d'usage afin que la communauté des entreprises innovantes puisse s'en saisir ;

– créer un guichet unique d'instruction des dossiers pour la participation à ces « bacs à sable » « *avec contrainte de délai de réponse* ».

Pour les rapporteurs, les recommandations du rapport précité de notre collègue Cédric Villani concernant l'intelligence artificielle sont, pour une large partie, applicables aussi à l'ensemble des développements innovants dans les technologies numériques. Les efforts mis en œuvre par le ministère des Armées pour se rapprocher des entreprises innovantes, notamment avec la création de « labs », vont dans ce sens et méritent d'être amplifiés dans le sens prôné par le rapport précité.

iii. Les liens entre la DGA et l'industrie

Plusieurs des interlocuteurs de la mission d'information ont regretté que les ingénieurs de la DGA, recrutés au meilleur niveau qui soit, ne puissent pas, dans le cours de leur carrière, effectuer des allers-retours avec le monde de la recherche et, surtout, avec celui de l'industrie.

Or les ingénieurs de la DGA sont statutairement des officiers de carrière. Interrogée sur cette idée d'assouplir leurs parcours de carrière pour favoriser des mobilités dans l'industrie, la directrice de la stratégie de la DGA a reconnu que les règles statutaires actuelles peuvent constituer un frein à des parcours très variés, mais que de **sérieuses questions de déontologie appellent une certaine prudence** dans l'étude de telles idées.

Pour les rapporteurs, il est en effet difficile d'envisager, dans des conditions compatibles avec les exigences déontologiques, des mobilités d'officiers de la DGA au sein de sociétés de droit privé qui se trouvent être cocontractantes du ministère des Armées. La question pourrait mériter un examen approfondi s'agissant de détachements dans le secteur de la recherche publique, tout en gardant à l'esprit que les industriels de la défense soutiennent parfois les laboratoires concernés.

c. L'innovation participative

L'un des aspects souvent mis en avant des démarches modernes d'innovation tient à l'encouragement des idées nouvelles formulées par les personnels mêmes d'une organisation. On parle alors d'« innovation participative » et, lorsque les personnels en questions sont fortement engagés dans le développement de projets validés, d'« intrapreneurs ».

Le ministère des Armées n'a pas attendu la « révolution numérique » pour soutenir l'innovation participative. En effet, depuis plus de vingt-cinq ans, la DGA a constitué en son sein une **mission « innovation participative »** chargée de recueillir et, le cas échéant, de soutenir, les idées innovantes de tout personnel des

armées ou de la gendarmerie, quels que soient son grade et son statut. Elle apporte à ces porteurs de projets un **soutien financier** – jusqu'à quelques dizaines de milliers d'euros – ainsi que **technique, administratif et juridique** – notamment en matière de droit de la propriété intellectuelle. Les prototypes sont réalisés soit par l'innovateur lui-même, soit par une entreprise à laquelle il confie cette tâche, en général une PME. Cette mission soutient une cinquantaine de projets par an.

Les projets soutenus couvrent un vaste champ d'usages, du véhicule de reconnaissance automatisé multitâche et à forte mobilité au sac de récupération des corps en milieu aquatique, du dispositif de fiabilisation de la saisie de données anthropomorphiques à la plaque permettant d'ériger une antenne sur un véhicule sans recours aux haubans, du programme informatique permettant aux chasseurs de mines d'utiliser le GPS au système laser pour le réglage du FAMAS. La réalisation la plus emblématique des dernières années est certainement Auxylium, le système précité de télécommunications sécurisées sur *smartphone* pour les actions de combat et de sécurité, qui a été généralisé à l'occasion de l'opération Sentinelle. Le capitaine Jean-Baptiste Colas, son développeur, a expliqué la genèse de ce projet, que résume l'encadré ci-après.

La genèse d'Auxylium,
programme emblématique de la démarche d'innovation participative

Après avoir intégré l'École nationale des sous-officiers d'active en 2005, Jean-Baptiste Colas a été affecté au 28e régiment de transmissions, affectation dont il a expliqué qu'elle l'avait sensibilisé dès le début de sa carrière aux spécificités de l'ouverture de théâtre et au problème du poids des matériels. Admis à l'École militaire interarmes en 2009, il a été chargé d'une mission sur le codage des transmissions et choisi, pour son projet de fin d'études, de travailler sur la numérisation du combattant – l'idée étant **d'alléger le système Félin**, dont les interfaces de communication sont peu intuitives et peu ergonomiques, encombrantes et difficiles à utiliser en réseau urbain dense.

C'est dans ce cadre qu'est née l'idée d'Auxylium, développé à deux officiers et présenté au ministre Gérard Longuet et au chef d'état-major de l'armée de terre Elrick Irastorza, qui ont soutenu le projet. Lorsqu'il poursuivait sa formation à l'école d'application de l'infanterie à Draguignan, Jean-Baptiste Colas a poursuivi le développement du système et sollicité à cet effet, sur le conseil et l'intervention du cabinet du chef d'état-major de l'armée de terre, une subvention de la **mission « innovation participative »** de la DGA.

La mission « innovation participative » lui a attribué 80 000 euros et la DGA l'a **mis en relation avec Atos** pour fabriquer des prototypes.

À l'issue de sa scolarité à l'école d'application, l'armée de terre a offert la possibilité au lieutenant Jean-Baptiste Colas de rester à Draguignan et de n'exercer les fonctions de chef de section qu'à temps partiel, pour pouvoir poursuivre le développement d'Auxylium. Ainsi, **l'armée de terre a soutenu cette innovation par une mesure adaptée de gestion des ressources humaines**.

En 2014, le projet a reçu le « prix de l'audace » du ministère ; il a donné lieu au développement de plusieurs prototypes expérimentaux en 2014 et 2015. Puis, en 2015, Jean-Baptiste Colas a été mis pour emploi à la DGA comme officier de programme – chargé de l'expression des besoins des armées – et conseiller pour l'innovation. Depuis le 1er janvier 2018, il est chef du bureau de la transformation digitale à l'état-major des armées.

Le déclenchement de l'opération Sentinelle a conduit à accélérer le programme de deux ans environ. Le 13 novembre 2015, Auxylium achevait à 20 heures une phase de tests et, le lendemain, il a été érigé du statut de projet de la mission « innovation participative » en « urgence opérationnelle », c'est-à-dire en « *mini-programme d'armement mené tambour battant, avec une concentration des ressources* » et bénéficiant de 32 millions d'euros pour la dotation de l'ensemble des unités Sentinelle de l'Ile de France, équipement compris. Le programme est appelé à être élargi à trois autres villes en 2018. Pour des raisons de hiérarchisation des charges industrielles, ce type de programme coûte en général 40 à 50 % de plus qu'un programme classique, mais permet de combler en urgence des lacunes capacitaires handicapantes en opération.

La conduite du programme a mobilisé jusqu'à 150 personnels chez Atos, quatre à la DGA, trois à la section technique de l'armée de terre et un seul au sein de l'état-major de cette armée.

La démarche d'innovation participative peut être encouragée notamment à l'occasion de la mise en service de nouveaux équipements, dont les personnels doivent s'approprier les possibilités et, à cette occasion, affiner les usages. C'est ce qu'a fait valoir le général Bernard Barrera s'agissant des matériels de la gamme SCORPION. Si ce mode de pilotage est « *peu naturel dans des organisations hiérarchisées comme les armées* », il a jugé intéressant de « *faire du transversal* », soulignant l'occasion que constitue pour cela l'opération SCORPION, qui « *crée une dynamique physiquement tangible favorable à la transformation et à l'innovation "*bottom up*"* ». Ainsi, « ***SCORPION arrivant, c'est l'occasion d'imaginer de nouveaux usages et d'appeler aux idées nouvelles*** ».

Lors d'un colloque organisé en décembre 2017 à l'École polytechnique, les rapporteurs ont pu se faire présenter par leurs inventeurs plusieurs équipements dont le développement a été soutenu par la mission « innovation participative ». Tel est le cas, par exemple, de la station de travail médicale extra-hospitalière « MedPack » mise au point par le sergent-chef Samuel Mercier, infirmier urgentiste des Pompiers de Paris – et, depuis, lauréat du 117e concours Lépine. Le sergent-chef s'est félicité du soutien de la mission « innovation participative », qui gagnerait encore en efficacité, selon lui, si les promoteurs de projets validés par la DGA pouvaient bénéficier de quelques souplesses dans l'organisation de leur temps de travail et, surtout, si la DGA pouvait mettre à leur disposition un catalogue de partenaires industriels susceptibles de développer des prototypes.

d. L'innovation d'usage

L'un des aspects les plus prometteurs de l'innovation en dehors des grands programmes réside dans l'innovation dite « d'usage », c'est-à-dire la recherche de nouveaux usages pour un matériel ou une technologie existante, moyennant des développements limités.

Les rapporteurs ont pu étudier à Washington le fonctionnement et les travaux d'un service particulier du *Department of Defense* : le ***Strategic Capabilities Office***, qui a pour cœur de métier la recherche de nouveaux usages pour les technologies existantes et que présente l'encadré ci-après.

Le *Strategic Capabilities Office*

1./ Le rôle du *Strategic Capabilites Office*

M. William Roper, directeur du *Strategic Capabilites Office*, a expliqué aux rapporteurs que la mission du SCO se distingue de celle de la DARPA en ce qu'à la différence de l'Agence, qui développe des technologies mais pas des équipements, **le *Strategic Capabilites Office* n'a pas pour mission de faire des découvertes technologiques, mais d'adapter les technologies existantes pour en faire des capacités militaires**. Il a illustré cette différence par l'exemple suivant : si la DARPA mettait au point un nouveau laser, c'est le SCO qui pourrait essayer d'en faire une arme. La DARPA démarre un projet sur une idée nouvelle, le SCO démarre un projet à partir d'un équipement existant.

Le *Strategic Capabilites Office* conduit ainsi ses programmes de R&D à partir de technologies qui existent déjà – qu'elles soient civiles ou militaires –, ce qui constitue une contrainte en soi. Beaucoup de ces technologies sont issues des travaux de la DARPA. L'enjeu, dès lors, consiste à la fois à trouver à ces technologies un usage « *surprenant* », utile aux forces armées, et à développer une capacité rapidement. Aux dires de M. William Roper, le but est de « ***répondre à 90 % d'un besoin dans des délais très courts plutôt quà 100 % du même besoin en dix ans*** ».

Le *Strategic Capabilites Office* fournit aux armées des prototypes et discute avec elles de leur appréciation sur le matériel. Son directeur a souligné le caractère « *participatif* » de cette procédure, qui place ce service à la charnière du monde de la R&D et de celui des « opérationnels ».

2./ Les moyens du *Strategic Capabilites Office*

Le service est organisé de façon à répondre à deux enjeux : garantir une certaine agilité au service, et favoriser les partenariats, car « *on n'innove pas seul dans son coin* ». Ainsi, le SCO est doté d'une équipe restreinte – 70 personnels –, le directeur insistant sur la pertinence de ce format, qui permet de :

– **se passer de tout encadrement intermédiaire** entre la direction et les chargés de programmes, facteur d'agilité dans la gestion du service ;

– « ***croiser les regards*** » et renouveler régulièrement les idées et les compétences ;

– obliger le service à **tisser des partenariats**, tant avec les armées qu'avec les services compétents des puissances alliées (ce sur quoi M. William Roper a insisté).

Le SCO gère un budget de 1,5 milliard de dollars par an.

3./ Exemples de projets conduits par le *Strategic Capabilites Office*

M. William Roper a cité plusieurs dossiers d'études représentatifs du travail du *Strategic Capabilites Office* :

– un projet consistant à exploiter les technologies de transmissions afin de mettre des équipements de toute nature (« capteurs » ou « effecteurs ») en réseau avec une capacité que les forces armées préfèrent ne pas trop exposer au feu, soit parce qu'il s'agit d'humains, soit parce qu'il s'agit d'équipements coûteux. Ce projet, appelé « ***Ghost Fleet*** », prévoit de disposer, autour d'une frégate, diverses plateformes navales moins coûteuses et autonomes ;

– doter les forces de **drones civils**, afin de bénéficier des développements rapides de l'industrie privée dans ce domaine, tout en assurant l'intégrité de ces systèmes en les dotant d'un **dispositif de destruction à distance** pour le cas où les forces en perdraient le contrôle ;

– développer des **logiciels personnalisables** à partir des logiciels civils, ce pour quoi le directeur du SCO a jugé que le *Department of Defense* n'a pas fait assez. Cette démarche poursuit à la fois des objectifs d'attractivité des équipements militaires pour les jeunes recrues « *digital natives* », et des objectifs d'efficience, considérant qu'il y a une forme de redondance à développer des logiciels pour les forces armées lorsque des logiciels du commerce remplissent les mêmes fonctions ;

– utiliser les technologies de ***blockchain*** : sécuriser ainsi les données elles-mêmes permet d'utiliser des réseaux moins sécuriser pour les transmettre. Le recours à la *blockchain* constituerait ainsi un changement de posture dans les moyens de sécurisation des transmissions, qui reposent aujourd'hui pour l'essentiel sur une logique de défense périmétrique, c'est-à-dire de pare-feu (*firewall*). M. William Roper a d'ailleurs fait valoir que ce changement est déjà à l'œuvre dans l'industrie financière.

L'existence de ce service est restée longtemps classifiée, mais une plus grande publicité est faite aujourd'hui à ses travaux et permet d'en mesurer l'intérêt. Une part de son apport à l'innovation réside dans l'utilisation au sein d'une armée d'équipements développés pour une autre ; la dimension interarmées de la DGA devrait permettre d'intégrer ces possibilités *ab initio* dans les programmes. Mais dans d'autres de ses travaux d'innovation d'usage, le *Strategic Capabilities Office* parvient à des résultats suffisamment intéressants pour qu'il paraisse pertinent de rechercher à s'en inspirer en France, par exemple à l'occasion de la création annoncée d'une agence de l'innovation de défense.

e. La culture de l'expérimentation et l'acceptation de l'échec

Comme l'a bien souligné le général Bruno Maurice, l'une des caractéristiques des modes modernes de pilotage de l'innovation réside dans « ***l'acceptation de l'échec comme voie possible d'apprentissage*** », pourvu que les délais dans lesquels sont conduits les projets soient suffisamment courts pour éviter que l'on s'enlise dans une voie infructueuse. Tel est d'ailleurs une des leçons de méthode que l'on peut tirer du travail de la DARPA.

Dans cette démarche « *nécessairement exploratoire* », l'échec doit être admis car il est source d'enseignement. Pour le général, « *on peut d'ailleurs se poser la question de la capacité de la DGA à intégrer ce nouveau type d'approche alors que sa culture et son ADN sont la conception et la conduite de programmes, de trente ans découlant de la dissuasion pour lesquels le "risque zéro" était la règle absolue* ».

L'aversion au risque dans les acquisitions du ministère des Armées peut aussi s'expliquer, comme dans d'autres ministères, par des **questions juridiques de responsabilité** : l'acheteur est d'autant moins enclin à choisir des produits innovants, donc plus risqués, si un échec s'avérait pénalisant pour lui. Pour parer des risques de ce type, tant quant aux produits achetés qu'aux procédures choisies pour régir leur acquisition, le rapport précité de notre collègue Cédric Villani fait une double recommandation :

– **rendre officielle la prise de risque demandée à l'acheteur** par sa hiérarchie, « *afin qu'un échec ne soit pas pénalisant* » ;

– établir un **régime de « *responsabilité en cascade* »**, où la responsabilité de l'État pourrait être recherchée en priorité, sauf à prouver une malveillance ou un abus délibéré.

En tout état de cause, l'innovation de rupture a toujours pour corolaire un risque d'échec, qu'il faut « dédramatiser » dans les pratiques administratives.

Les administrations ne sont apparemment pas les seules organisations en France à présenter un degré élevé d'aversion au risque. Comme l'a fait observer un haut responsable d'un service de renseignement, en France, peu de *start-up* déposent le bilan ; paradoxalement, il n'y a pas lieu de s'en féliciter, car ce constat ne s'explique pas seulement par l'excellence de ceux qui créent des *start-up*, mais par le fait qu'il s'en crée moins, signe d'une certaine aversion au risque sinon chez les entrepreneurs, du moins dans l'industrie du capital-risque.

3. Stimuler l'écosystème de recherche et d'innovation suppose de moderniser les procédures et les pratiques d'acquisition d'armements

Les rapporteurs ont observé un large consensus parmi les acteurs de l'écosystème de recherche et d'innovation intéressant la défense pour estimer que les procédures actuelles d'acquisition d'armement – et la pratique qui en est faite depuis une vingtaine d'années – sont davantage adaptées aux « grands » programmes qu'aux « petits ». Or les innovations dans le champ numérique se traduisent le plus souvent par des programmes d'importance financière limitée en comparaison des « grandes » opérations d'armement, mais aussi par des progrès technologiques qui se succèdent à un rythme soutenu – qui imaginerait conserver un système d'information aussi longtemps qu'une frégate ou qu'un blindé ?

Les dispositifs de contournement mis en œuvre jusqu'à présent par la DGA pour capter l'innovation numérique, principalement auprès des petites et moyennes entreprises, sont utiles à cet égard et méritent d'être poursuivis et encore adaptés à certaines spécificités des *start-up*.

a. Les procédures d'acquisition méritent d'être adaptées au rythme de plus en plus soutenu de l'innovation numérique

Comme l'a relevé l'officier général chargé de la transformation digitale des armées, la transformation digitale doit pouvoir « *être pilotée par les délais* », car l'innovation numérique nécessite de s'approprier des technologies « *en quelques mois* » puis d'en industrialiser la production et la dotation aux forces dans les meilleurs délais.

i. Pour les « petits » programmes innovants, les procédures classiques sont généralement vues comme insuffisamment « agiles »

La plupart des acteurs entendus par les rapporteurs jugent que les délais résultant des procédures d'acquisition d'armements de droit commun, décrites par l'instruction générale n° 125/1516 du 26 mars 2010 [(1)] – « la 1516 » –, sont trop longs au regard du rythme de l'innovation dans le secteur du numérique. Ce décalage tend à structurer le marché de l'armement de façon plus duale qu'auparavant, avec un contraste plus net entre, d'une part, des produits innovants pour lesquels les cycles d'innovation sont très courts, nourris par la vitalité des PME et des *start-up* et, d'autre part, les plateformes majeures fournies par les « grands » industriels, appelées à rester en service plusieurs décennies.

- *Les délais de mise en œuvre des procédures d'acquisition « classiques » se trouvent en décalage avec le rythme aujourd'hui soutenu de l'innovation technologique*

Les représentants du Comité Richelieu ont observé que, globalement, **il faut aujourd'hui une vingtaine d'années pour l'intégration d'une technologie émergente**. Il faut en effet « *deux ou trois ans de R&D* » financés par un programme d'études amont, puis « *un long travail d'écriture des spécifications* » d'un marché par la DGA, puis un appel d'offres, des prototypes et des démonstrateurs, avant qu'un programme d'équipement soit lancé et se traduise par de nouvelles dotations à grande échelle dans les forces.

Or ce rythme est **incompatible avec le *tempo* de l'innovation numérique, ou de manière plus générale l'accélération des cycles technologiques** : à cet égard, même le délai moyen de deux ans pour l'aboutissement d'un appel d'offres est parfois trop long pour que la technologie visée par les spécifications administratives ne soit pas dépassée par des développements plus innovants intervenus entre-temps. Ainsi, l'organisation en grands programmes de défense, suivant « la 1516 », n'est guère adaptée à l'économie numérique, ni à l'intégration des innovations technologiques dans les grands programmes d'armement.

Outre les délais, d'autres paramètres réglementaires sont souvent vus comme peu adaptés à la « révolution numérique ». Ainsi, tant en France que dans d'autres pays, comme les rapporteurs ont pu le constater par exemple aux États-Unis, ces règles d'achat public sont faites de façon à limiter le risque technologique. À cette fin, les procédures conduisent à enserrer l'usage opérationnel d'une technologie dans une définition précise dès un stade précoce du projet – les stades d'orientation et d'élaboration d'un programme au sens des points 4.2 et 4.3 de l'instruction ministérielle 125/1516 précitée. Or, comme l'ont fait valoir les représentants d'IBM interrogés à Washington par les rapporteurs, **démontrer l'utilité opérationnelle d'un concept** – « *Proof of Concept* » dans le

(1) Instruction générale n° 125/DEF/EMA/Plans/COCA – n° 1516/DEF/DGA/DP/SDM relative au déroulement et la conduite des opérations d'armement, en date du 26 mars 2010.

droit américain – **dès le début du programme n'est pas toujours possible pour des applications nouvelles**, comme l'intelligence artificielle ou le *big data*.

En outre, les procédures d'acquisition ne sont pas nécessairement allégées en fonction du coût du programme concerné. C'est ce qui fait dire aux *start-up* et aux militaires rencontrés par les rapporteurs au « DGA Lab » que l'effort requis pour mettre en place un circuit de commandes et de livraison est lourd par rapport au faible coût des prestations des *start up* : « *pour 15 000 ou 20 000 euros, c'est à peu près la même procédure que pour 20 millions d'euros* ».

Les rapporteurs relèvent d'ailleurs que contrairement à une apparence de grande maîtrise de la « révolution numérique » par les armées américaines, les procédures d'acquisition du *Department of Defense* sont souvent critiquées pour leur manque de souplesse – plus encore qu'en France celles de la DGA. D'ailleurs, les principaux programmes américains de traitement automatisé des informations (*Major Automates Information Systems*) ont connu d'importants dérapages financiers et calendaires, et la culture de la prise de risque n'est pas si développée qu'on pourrait le penser dans l'ensemble des services du Pentagone.

- *Un passage à faciliter du stade de l'expérimentation à celui de l'industrialisation*

L'une des leçons que l'on peut tirer de l'émulation récente au sein du ministère des Armées autour de projets innovants tient à leur devenir, c'est-à-dire à l'industrialisation des produits expérimentés avec succès. L'amiral Arnaud Coustillière a fait observer qu'à cet égard, conduire des expérimentations n'est pas l'opération la plus compliquée ; « *l'enjeu, c'est l'industrialisation* ».

Or il ressort des différents « défis », « projets "éclaireurs" » et « labs » que **c'est dans le financement du passage du stade de l'expérimentation à celui de l'industrialisation que naissent les plus grandes difficultés**.

Il en est ainsi, à titre d'exemple, des projets « éclaireurs » de l'armée de terre étudiés par les rapporteurs au 12e régiment de cuirassiers. Selon le colonel Olivier Kempf, l'industrialisation de l'ensemble des projets « éclaireurs » et des chantiers de la transformation digitale – c'est-à-dire leur généralisation à l'ensemble des militaires de l'armée de terre – demanderait un investissement de trois à quatre millions d'euros par an pendant quelques années de montée en puissance, pour l'acquisition de divers objets connectés, de différents capteurs, d'une plateforme de service sur Internet, d'applications et d'API, ainsi que de nouvelles technologies comme le *big data* ou la *blockchain*. Cependant, aucune ligne budgétaire n'a été ouverte à cet effet.

Or des expérimentations sans lendemain peuvent avoir un effet démobilisateur. Comme l'a fait remarquer le directeur du renseignement militaire, « *"allécher" les services par des produits qu'ils ne pourraient pas acquérir serait inutile, voire contre-productif* ».

Par ailleurs, il ressort des entretiens des rapporteurs avec les militaires des armées et du commissariat des armées rencontrés au « DGA Lab » que **l'accès aux compétences de la DGA en matière de contractualisation n'est pas aisé pour les « opérationnels »**, même lorsqu'ils nouent des liens prometteurs avec des *start-up*. L'ingénierie contractuelle de la DGA constitue un savoir-faire précieux, dont tous les organismes du ministère des Armées auraient besoin. Ce constat se traduit par des difficultés dans le passage du stade de la « preuve de concept » à échelle industrialisée.

- *Vers une « dualisation » des marchés d'équipement des forces ?*

Nul ne remet en question la pertinence de « la 1516 » ou l'expertise de la DGA en elles-mêmes. D'ailleurs, comme l'a souligné le général Bernard Barrera, alors sous-chef d'état-major de l'armée de terre chargé des plans et des programmes, **« la 1516 » est parfaitement adaptée au développement de plateformes complexes et la DGA gère très efficacement ces grands programmes**, en leur garantissant une cohérence d'ensemble sans équivalent dans le monde – notamment à notre niveau de ressources budgétaires.

Mais, dans le même temps, il a considéré que **les projets de réforme des procédures d'acquisition évoquée par la ministre des Armées sont bienvenus pour des équipements plus légers**, tels que des systèmes d'information, des drones et de petits matériels dits « de cohérence ». Pour intégrer ces technologies nouvelles, développées notamment par des *start-up* et des PME, une expression de besoins dans les conditions de « la 1516 » constitue une procédure inadaptée.

Il semble aux rapporteurs que la difficulté soit cependant moins liée à la taille de l'entreprise fournisseur qu'aux pratiques de l'économie numérique elle-même ; en effet, les « GAFA » n'ont plus rien de *start-up*. Et pourtant, comme l'a relevé à titre d'anecdote le général Bruno Maurice, le commandant suprême de l'OTAN pour la transformation a bien essayé de prendre attache avec les « GAFA », mais tous ont marqué de sérieuses réticences lorsqu'il s'agit de travailler de façon étroite avec ses services, car ceux-ci ne sont pas vus comme étant assez « agiles ».

Le ministère des Armées a donc intérêt à prendre en compte les pratiques spécifiques de ce secteur technologique. Il commence d'ailleurs à le faire, par exemple en matière de SIAG. M. Paul Serre a en effet expliqué que le SGA opère déjà, en réalité, deux canaux de pilotage de ces programmes :

– une commission des SIAG réunit l'ensemble des autorités du ministère ; elle anime les projets de systèmes d'information et propose des arbitrages entre les besoins et les ressources, suivant des logiques classiques de direction de projet ;

– en parallèle, existent plusieurs projets d'innovation, souvent participative, visant des résultats souvent plus simples, parfois plus concrets, et suivant des méthodes généralement plus « agiles ». Ainsi, début 2017, le SGA a lancé un « défi d'idées » et recueilli une centaine d'idées nouvelles, « *d'inégal*

intérêt, mais d'où sont ressorties neuf idées majeures et six projets », certains en partenariat avec des *start-up*.

M. Paul Serre a souligné que ces deux canaux sont « *naturellement distincts, mais indissociables* », ne serait-ce que parce que même des projets « agiles » doivent s'intégrer à l'écosystème complexe du ministère des Armées.

Plus généralement, on peut voir le développement des « labs » et campus précités dans les différentes armées, directions et services comme participant de la même logique de dualisation des modes de pilotage des acquisitions du ministère.

ii. Pour les « grands » programmes et les systèmes d'information, l'intégration de l'innovation en cours de développement et tout au long de leur durée de service constitue également un enjeu

Illustration du décalage entre le rythme de l'innovation numérique et la durée de développement des grands équipements, un des interlocuteurs des rapporteurs a raconté qu'à l'entrée en service de la frégate *Chevalier Paul*, en 2011, certains personnels étaient surpris que les postes de télévision livrés fussent dotés de tubes cathodiques. En effet, la commande passée onze ans plus tôt n'intégrait pas les avancées de la technologie intervenues entre-temps. Si elle peut sembler futile, cette anecdote montre que même dans les « grands » programmes d'armement, l'intégration des développements rapides des technologies numériques mérite d'être mieux assurée, à la fois pendant le développement des équipements et pendant leur durée de service.

- *Établir des spécifications en termes fonctionnels ou capacitaires plutôt que techniques faciliterait l'intégration de l'innovation aux « grands » projets d'équipement*

Pendant la phase de développement des matériels, il convient pour ce faire **que les spécifications des contrats d'armement soient le plus souvent possible rédigées en termes de capacités à fournir** – à charge pour l'industriel de trouver la technologie la plus adaptée – **plutôt qu'en des termes techniques précis, contraignants dans le choix des technologies**, et supposant donc de longues négociations d'avenants pour intégrer des technologies plus récentes, d'ailleurs souvent moins onéreuses que celles qu'elles remplacent.

En effet, les pratiques en matière de spécification des équipements dans les programmes d'armement peuvent être adaptées de façon à faciliter l'intégration des développements technologiques en cours de conduite d'un « grand » programme d'armement. Ces spécifications sont généralement énoncées par la DGA en des termes techniques contraignants, ce qui a pour effet d'enserrer les développements dans des critères très stricts, ne permettant pas de tirer profit de technologies nouvelles qui permettraient de remplir la même fonction ou de conférer aux forces la même capacité. Comme l'a fait valoir le président du GICAT, il s'agit de recourir davantage aux techniques civiles et de passer d'une

logique de développement *ex nihilo* d'un armement suivant des spécifications précises à une logique d'intégration rapide de technologies nées dans le civil.

Les représentants du GICAN ont cité comme exemple le cas du « pod orientable », élément de propulsion maritime qui remplace à lui seul le couple hélice–gouvernail : la DGA spécifiait auparavant les caractéristiques techniques des hélices et des gouvernails, et s'est trouvée démunie devant la nouveauté que constituent ces « pods ».

Ainsi, **énoncer les spécifications en termes fonctionnels ou capacitaires pourrait faciliter l'intégration des innovations en cours de développement d'un équipement complexe**.

Pa ailleurs, les représentants de Thales ont aussi estimé qu'une « ***maîtrise des spécifications*** » peut aussi concourir à une politique industrielle efficace. À l'appui de leur propos, ils ont cité l'exemple suivant : l'État avait envisagé de modifier les PR4G pour les doter de protections supplémentaires, mais Thales a plaidé contre, faisant valoir que le PR4G perdrait en compétitivité sans que le gain capacitaire pour les forces soit très conséquent.

- *La démarche incrémentale facilite l'intégration de l'innovation, pourvu que l'architecture des équipements soit suffisamment ouverte* ab initio

Le développement incrémental, consistant à intégrer des innovations technologiques tout au long du cycle de vie d'un équipement, permet de concilier les durées de service très longues des plateformes majeures et le rythme de l'innovation. D'ores et déjà, cette démarche de développement incrémentale a été adoptée pour plusieurs équipements – tels les hélicoptères Tigre ou les avions Rafale –, et selon la plupart des observateurs, **les cycles de mise à jour pourraient encore être raccourcis**.

De même, la démarche incrémentale mérite d'être privilégiée y compris pour des équipements moins onéreux ou moins emblématiques, mais soumis à des évolutions technologiques rapides, tels les **systèmes d'information**. L'amiral François Moreau a donné un exemple très parlant de l'intérêt opérationnel que peut revêtir une mise à jour régulière de ces systèmes : même sans modification du matériel « physique » des sonars, le mode de traitement du signal compte pour 60 % à 70 % de la performance de l'équipement, et c'est ainsi que la marine a réussi à doubler la portée des sonars sans changer d'équipement physique.

En outre, l'adoption rapide des développements technologiques innovants revêt un intérêt non seulement opérationnel, en ce qu'elle confère une supériorité à nos systèmes d'armes, mais aussi financier, en ce que l'entretien de technologies et de compétences dépassées a un coût élevé. Ce facteur joue particulièrement pour les programmes numériques. En effet, la rapidité de l'innovation en la matière se traduit par des changements de standards dont le rythme est soutenu.

Ainsi, **le rythme de l'innovation appelle aujourd'hui un système de modernisation « tout au long de la vie » et non plus seulement « à mi-vie »** des plateformes majeures comme des autres équipements. Cette exigence est d'ailleurs cohérente avec le système de « contrats globaux » que tend à privilégier la DGA, consistant à négocier dans le même temps l'acquisition d'un matériel et son maintien en condition opérationnelle à long terme.

Cette démarche incrémentale suppose aussi **que l'architecture physique comme informatique des plateformes soit suffisamment « ouverte »** pour intégrer l'innovation, tout en restant suffisamment maîtrisée pour garantir la sécurité des systèmes d'armes. Cette logique a été mise en œuvre, par exemple, pour la frégate de taille intermédiaire.

- *L'hiatus entre acquisition et MCO est préjudiciable à la bonne gestion des systèmes d'information pendant tout leur cycle de vie*

Comme l'ont souligné les responsables de la R&D de Naval Group, dans les procédures du ministère des Armées, acquisition et MCO sont systématiquement traités séparément, alors qu'**avec le numérique, le cycle de vie d'un produit prend de plus en plus d'importance**.

Cette disposition ne permet ni d'exploiter au mieux les éléments de transversalité entre les différents programmes, ni d'innover dans le MCO car, par une habitude hélas fréquente, l'investissement dans le MCO d'un équipement fait régulièrement l'objet de renoncements consentis afin de dégager les ressources financières nécessaires à son acquisition, compte tenu des contraintes budgétaires.

b. Les dispositifs de contournement des procédures classiques méritent d'être approfondis et encore adaptés, notamment aux start-up

i. La DGA a d'ores et déjà mis en œuvre des dispositifs de contournement des procédures et pratiques classiques, en faveur des PME

Les rapporteurs soulignent que la DGA ou le ministère des Armées dans son ensemble ont d'ores et déjà mis en œuvre un large éventail de moyens visant à pallier – ou à contourner – les difficultés que rencontrent les entreprises technologiques innovantes dans la mise en œuvre des procédures d'acquisition classiques, en vue de faciliter l'intégration par les forces et leurs soutiens des technologies nouvelles issues de la recherche et développement duale ou, de plus en plus souvent, civile. Schématiquement, ces dispositifs s'analysent soit comme des procédures financières dérogatoires, soit comme des organisations administratives nouvelles – les « labs » et autres campus – visant à favoriser les contacts entre le ministère et les entreprises innovantes autres que ses grands cocontractants habituels.

- *Des dispositifs financiers de soutien à l'innovation destinés aux PME, aux start-up voire aux personnels du ministère eux-mêmes*

Comme l'a expliqué sa directrice de la stratégie, la DGA a d'ores et déjà mis en œuvre plusieurs dispositifs de soutien à l'innovation alternatifs aux programmes d'études amont – confiés le plus souvent à de grands industriels. Elle a cité à ce titre :

– le soutien aux projets scientifiques financés *via* l'Agence nationale de la recherche (ANR) au titre du programme d'accompagnement spécifique des travaux de recherches et d'innovation pour la défense (**ASTRID**), pour huit millions d'euros par an ;

– le financement de prototypes en aval des projets financés *via* le mécanisme ASTRID, dans le cadre du dispositif « **ASTRID maturation** », pour quatre millions d'euros par an ;

– le régime d'appui aux PME pour l'innovation duale (**RAPID**), qui participe au fonds unique interministériel et aux pôles de compétitivité sous l'égide de la direction générale des entreprises (DGE) du ministère de l'Économie. Mme Caroline Laurent a assuré que si cet outil est parfois remis en cause, dans un mouvement de refonte des dispositifs soutien à l'innovation, la DGA souhaite le conserver car il lui permet de mieux connaître l'écosystème des PME et d'entretenir avec elles des liens, au-delà des seules PME auprès desquelles la DGA passe des contrats d'acquisition. Les représentants du comité Richelieu ont dressé un bilan très positif de ce dispositif depuis son renforcement en 2013 dans le cadre du « Pacte Défense PME », qui a prévu que le montant des crédits alloués passerait de 10 millions d'euros à 50 millions d'euros par an. À leurs yeux, ce dispositif est « *bien adapté au modèle économique des* start-up *et des PME innovantes* » ;

– la « **mission innovation participative** » (MIP) de la DGA, qui finance des projets innovants coûtant moins de 90 000 euros. Certes, le dispositif est réservé aux militaires, mais ceux-ci peuvent s'associer à des PME pour développer leurs innovations. D'ailleurs, selon les représentants du comité Richelieu, les militaires de la « *génération* start-up », qui forment « *un vivier bouillonnant* », se tournent assez spontanément vers les PME ;

– la création de « **Définvest** » en novembre 2017, fonds d'investissement qui spécialisé dans le soutien aux entreprises innovantes non pas par des subventions, mais par des apports en capital (en fonds propres et en « quasi-fonds propres ») opérés par la Banque publique d'investissement (BPI). Le fonds pourrait être abondé à raison de 10 millions d'euros par an, pour atteindre 50 millions d'euros à terme : cette voilure financière est certes limitée, mais la DGA compte sur les effets de levier que pourraient avoir ces investissements.

Selon les précisions fournies par le président Jean-Jacques Bridey dans son rapport sur le projet de loi de programmation militaire pour les années 2019 à 2025 [(1)], le fonds Definvest interviendra en effet conjointement avec d'autres investisseurs du secteur privé et conservera toujours une position minoritaire. Il conduira soit des opérations de capital-risque pour les entreprises jeunes et innovantes, soit des opérations de capital-développement pour les « *entreprises établies cherchant à croître* ». Les sociétés bénéficiaires de ces appuis seront sélectionnées en fonction de l'importance de leurs innovations, connaissances ou savoir-faire pour à la performance des systèmes de défense français ou la place de l'industrie française dans les marchés mondiaux. Selon le rapport précité, les équipes de la DGA et de BPI-France ont d'ores et déjà analysé une soixantaine de demandes et travaillent sur une dizaine de dossiers pertinents. Un premier investissement a été annoncé au mois d'avril 2018, et plusieurs autres devraient être opérés à partir de l'été 2018.

On citera également :

– les « **urgences opérationnelles** », régime dérogatoire aux règles d'acquisitions de droit commun qui permet aux armées d'acquérir des équipements « sur étagère » s'ils répondent à un besoin opérationnel non anticipé. Les représentants du comité Richelieu ont observé que s'il est « *très bon dans son principe* », ce régime passe cependant par une procédure d'appel d'offres, et donc de mise en concurrence, ce qui est « *trop lourd pour certaines* start-up » ;

– le dispositif des « **achats publics innovants** », par lequel l'État, ses opérateurs et les établissements publics hospitaliers se sont engagés à consacrer en 2020 2 % du montant de leurs achats – qui représentent environ 60 milliards d'euros par an – à des produits innovants fournis par des PME. Les représentants du comité Richelieu ont jugé bon le principe de cet engagement, tout en en soulignant la modestie des objectifs fixés et en regrettant l'absence d'instruments de suivi. Un « guide pratique de l'achat public innovant » a certes été élaboré par le ministère de l'Économie et des Finances, mais le comité constate qu'il reste « *peu connu* ». Pour ses représentants, les freins sont d'ailleurs davantage d'ordre culturel que juridique. En effet, un marché public peut comporter des clauses liées à l'innovation pour un certain pourcentage de son montant, « *mais les acheteurs n'ont pas le réflexe d'en insérer* ». En outre, la catégorie des PME exclut les ETI, comme d'ailleurs certains autres dispositifs.

Le « **Pacte défense – PME** » prévoit aussi la passation de trente contrats d'études amont de moins de deux millions d'euros, donc *a priori* adaptés aux PME, même si, selon le comité Richelieu, cette mesure a été rarement mise en œuvre. Selon le comité, le plus important dans ce Pacte tient à « *un phénomène d'acculturation* ». En effet, « *M. Jean-Yves Le Drian avait suscité un engagement*

(1) Rapport n° 765 fait par le président Jean-Jacques Bridey au nom de la commission de la Défense nationale et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, mars 2018.

moral des grands groupes auprès des PME, et la DGA a examiné avec davantage d'attention les contrats de sous-traitance ».

La recherche de mécanismes de contournement des rigidités existantes dans les procédures d'acquisition de droit commun n'est pas le propre de la France. Aux États-Unis par exemple, un dispositif appelé *Other Transaction Authority* (1) permet des dérogations au droit commun des marchés publics américains, et le *Department of Defense* y a souvent recours.

- *Des organisations administratives innovantes : les « labs »*

Le resserrement des liens entre les entreprises innovantes, notamment pour les technologies civiles susceptibles d'avoir un usage dual ou des applications militaires, passe aussi par le développement de lieux de contact entre les armées, directions et services du ministère et les entreprises innovantes. Comme l'a expliqué le général Bernard Barrera, il s'agit de « *mécanismes de " boucle courte"* » vus comme « *sont nettement plus efficaces pour lier les* start-up *et les forces* », c'est-à-dire permettre à des industriels de faire des démonstrations de nouvelles capacités aux forces, tant conventionnelles que spéciales, puis de les expérimenter sur le terrain. Tel est l'objet des **divers organismes créés sous l'appellation de « labs »**, à l'instar du « DGA Lab » présenté plus haut.

L'officier général chargé de la transformation digitale des armées au sein de l'état-major des armées a souligné que ces organismes avaient permis des **contacts fructueux entre les forces et des *start-up***. Il a cité plusieurs projets qui ont connu un **débouché capacitaire**.

Ainsi, par exemple, des « défis » ont été organisés au sein du « DGA Lab » pour l'équipement des forces spéciales, le plus emblématique étant celui qui portait sur la question suivante : « quel serait l'apport d'un drone commercial dans une mission de libération d'otages de type *indoor* – capable de voler à l'intérieur de bâtiments –, suivant un scénario d'intervention comparable à une récente opération dans un hôtel de Bamako ? ». Quinze projets ont été déposés dans le cadre d'un dialogue avec les unités militaires concernées. Résultat : quinze équipes de projet ont été constituées, et les forces spéciales suivent ainsi de près la maturation des technologies concernées.

Autre exemple de réussite : l'exploitation de données satellitaires pour la surveillance maritime. Toutes les données utiles étant disponibles de façon ouverte, le défi tient à leur exploitation coordonnée. La DGA n'a pas porté le projet à l'étape du dialogue compétitif, préférant à défaut mettre en œuvre un contrat existant avec Thales et en décliner de nouveaux bons de commande. Pour le général Bruno Maurice, si Thales « *se met en mode "agile", il est pertinent de l'associer aux défis* ». Certes, ceux-ci sont initialement conçus pour les *start-up*,

(1) La National Defense Authorization Act *(NDAA) pour 2016 (section 845) confère au* Department of Defence *le droit de recourir à des procédures dérogatoires au droit commun des marchés publics du gouvernement fédéral pour l'acquisition de « prototypes » d'armes ou de systèmes d'armes.*

mais « *il faut pouvoir exploiter toutes les voies* », sans avoir de préférence pour telle ou telle catégorie d'industriels. À ses yeux, l'association de *start-up* aux « grands » groupes constitue une alternative intéressante, « *car elle permet de combiner l'agilité innovatrice du "petit" avec la capacité d'intégration et de passage à l'échelle industrielle du "grand"* ».

ii. Les dispositifs visant les PME méritent d'être encore adaptés, notamment aux spécificités des *start-up*

La directrice de la stratégie de la DGA a reconnu que **les divers dispositifs de contournement susmentionnés ne sont pas toujours les plus adaptés aux spécificités des *start-up***, dont le développement mérite encore d'être soutenu. Aussi, dans le cadre de son chantier de transformation, le ministère explore-t-il les moyens de soutenir davantage les *start-up*, par des participations en capital ou des acquisitions.

- *Assurer la cohérence et la lisibilité des différents « labs »*

Le général Bruno Maurice a reconnu que, fin juin 2017, il était apparu nécessaire de mettre en cohérence les écosystèmes de transformation digitale de chacune des armées. Si le foisonnement des initiatives au sein de chaque armée, direction ou service du ministère des Armées a contribué assurément à une profonde prise de conscience des enjeux de la numérisation des armées, ce foisonnement comporte deux risques :

– que des travaux ou des ressources rares, par exemple en matière de contractualisation ou de conduite des projets, soient inutilement dupliqués ;

– que cet ensemble, construit en entités différentes et propres à chaque armée, direction ou service, ne soit finalement guère plus compréhensible pour les entreprises innovantes que ne le sont les procédures classiques de la DGA.

C'est pourquoi un chantier de réflexion sur l'innovation a été lancé par la ministre des Armées en novembre 2017 et devrait déboucher prochainement, selon les précisions fournies par le président Jean-Jacques Bridey dans son rapport précité, sur « *de nouveaux outils favorisant l'expérimentation au sein des Armées et la relation avec les* start-up ».

Pendant la discussion du projet de loi de programmation militaire 2019-2025, la ministre a annoncé la **création d'une « agence de l'innovation de défense »**. Selon les précisions recueillies par les rapporteurs, cette mesure poursuit trois buts principaux :

– établir un système permettant d'intégrer une part de l'innovation technologique pour laquelle les programmes d'études amont s'avèrent peu adaptés, c'est-à-dire les technologies pour lesquelles **les délais d'appropriation sont plus courts, les barrières technologiques moindres et la stratégie du ministère orientée moins par une logique de planification des développements**

technologiques que par une logique « opportuniste », consistant à faire fond sur les innovations du secteur civil ;

– **associer davantage les armées** (c'est-à-dire les utilisateurs des équipements) et la DGA dans le pilotage de ce champ de développements technologiques ;

– étendre le champ des entreprises partenaires de la défense en **consolidant l'ensemble formé par les différents « labs »**, ce qui suppose de doter celui-ci d'un pilotage cohérent et de capacités qui lui manquent, notamment des expertises en matière de procédures d'achat et de conduite de projet.

Cette agence pourrait avoir un statut de service à compétence nationale et les quelques dizaines de personnels dont elle serait dotée pourraient être recrutés à la fois au sein des armées et de la DGA.

De façon cohérente avec la création de cette agence, le rapport annexé au projet de loi de programmation militaire 2019–2025 annonce la mise en place d'un « **Innovation Défense Lab** », qui sera la **tête de réseau des différents « labs »** existants. Selon les explications du général Bruno Maurice, la mise en place d'une telle tête de réseau vise à « *capter le foisonnement d'innovations et d'initiatives* bottom-up ». Colocalisé avec le « DGA Lab », l'« Innovation Défense Lab » a pour objet de « *mettre en œuvre l'innovation* » suivant un processus présenté comme celui « *des trois "i" : idéation* [(1)]*, incubation et industrialisation* ». L'encadré ci-après en présente les caractéristiques.

L'« innovation Défense Lab »

L'« Innovation Défense Lab » sera une structure du ministère des Armées, offrant des services aux armées, directions et services du ministère pour développer des projets innovants. Il aura pour mission d'« *interconnecter* » les différents « Labs » existants (notamment le DGA Lab, l'Armées Lab et le SGA Lab) « *dans un esprit de subsidiarité* ». Le ministère des Armées précise que « *cette fédération permettra la mutualisation des outils et moyens requis par tous les Labs spécifiques : gestion de communauté,* design thinking*, tiers lieu, achat rapide de maquettes, etc* ».

Le ministère des Armées présente les missions de cet organisme d'une façon résolument inspirée par le vocabulaire des *start-up* :

– « ***expérimenter et tester*** », c'est-à-dire « *manipuler des matériels existants ou adaptés* » et tester des idées et des schémas opérationnels pour « *contribuer à faire émerger l'innovation d'usage* ». Le rôle de l'iDLab sera « *d'être instigateur ou coordinateur des tests* », c'est-à-dire d'acquérir des prototypes « *de façon radicalement plus rapide qu'actuellement* », de proposer des prestations de soutien au test et d'en organiser un retour d'expérience. Il « *travaillera également à la fluidification de l'expérimentation "terrain" du ministère* », afin de « *mettre en relation l'idée avec son utilisateur final* » et, ce, « *dans un temps court* » ;

(1) Processus créatif de production, développement et communication de nouvelles idées.

– **organiser des événements**, tels des conférences et des démonstrations de produits, étant précisé que l'iDLab aura une «*fonction "ateliers de* co-working*"* » et servira aussi, « *par son tiers-lieu colocalisé, de "show-room" ministériel* » ;

– « ***mettre en réseau les intrapreneurs et les innovateurs****, en favorisant le co-working* », de façon à soutenir « *l'intraprenériat* » au sein du ministère.

Source : Rapport n° 765 fait par le président Jean-Jacques Bridey au nom de la commission de la Défense nationale et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, mars 2018.

Ce « Défense Lab » serait ainsi piloté par l'agence de l'innovation de défense. Aux yeux des rapporteurs, il serait cohérent que cette agence se voie également transférer la tutelle de la mission « innovation participative » de la DGA, avec laquelle d'évidentes synergies existeront, ainsi que, le cas échéant, le pilotage d'une part des programmes d'expérimentations technico-opérationnelles et des opérations d'expérimentation réactive.

- *Prendre en compte les spécificités financières des* start-up

Le soutien direct de l'État à une *start-up* peut être compliqué par la structure capitalistique de ce type d'entreprises. En effet, une aide d'État ne peut légalement avoir un montant supérieur au chiffre d'affaires annuel de son bénéficiaire. Or les *start-up* sont par nature en phase de croissance rapide de leur activité et beaucoup d'entre elles **commencent leur activité sur fonds propres, sans chiffre d'affaires**.

D'ores et déjà, le « DGA Lab » et les structures de même nature créées par les armées, directions et services du ministère des Armées permettent de mettre en œuvre un **mode de contractualisation innovant : les défis**, davantage adaptés aux jeunes entreprises innovantes que les procédures classiques. La mise en cohérence des différents laboratoires autour de « Défense Lab » doit permettre d'amplifier ce mouvement.

- *Contractualiser avec les PME ou, à défaut, garantir leur accès aux contrats dans des rapports de sous-traitance équilibrés*

Les représentants du comité Richelieu font valoir que la politique « massification » des programmes d'armement, suivie par la DGA depuis 1996, a eu pour effet de réserver *de facto* les contrats aux grands groupes ou, au mieux, à de grandes sociétés de services en ingénierie informatique. « *Les PME passent donc toujours après* », et n'accèdent le plus souvent aux marchés de la DGA que comme sous-traitants. Le comité Richelieu plaide donc depuis de nombreuses années en faveur d'une politique ambitieuse de contractualisation directe de la DGA avec les PME.

Cependant, fait valoir la DGA, **la contractualisation avec des *start-up* n'est pas toujours aisée pour des raisons d'interopérabilité et d'intégration de leurs technologies au sein des systèmes existants**. Selon sa directrice de la stratégie, le « défi image » récemment mis en œuvre l'a encore montré : Thales

fournissant déjà les 500 unités de traitement déployées par la DRM, la question de l'ajout d'un module de traitement particulier pose la question de son intégration dans le système existant. Le plus simple et le plus rapide a été d'inviter de manière pressante Thales à intégrer les technologies des *start-up* et à les mettre en place sur les équipements qu'il avait déjà fournis. Cette difficulté est particulièrement forte dans le champ des technologies numériques innovantes car, comme il ressort régulièrement des « rencontres INRIA–industrie », les standards informatiques ne sont pas harmonisés dans nombre de domaines technologiques encore en développement, comme celui des objets connectés.

Le principal problème qui résulte pour les *start-up* et autres PME de la position de sous-traitant tient à la propriété intellectuelle : « *les grands groupes la conservent quasiment toujours* », même si certaines avancées sont observées depuis la mise en œuvre du « Pacte défense PME ». Or, avec l'innovation numérique, la propriété intellectuelle est souvent le principal actif d'une *start-up*. Les rapporteurs ont d'ailleurs été interpellés sur cette difficulté par l'une des *start-up* dont ils ont rencontré les dirigeants au « DGA Lab ».

Pour la DGA, passer un contrat directement avec une *start-up* plutôt que *via* un des grands groupes avec lesquelles elle est régulièrement en affaires revient à prendre à sa charge une part de risque supplémentaire dans la conduite d'un projet d'armement. Néanmoins, selon les rapporteurs, **la DGA pourrait utilement assumer un tel risque et passer plus fréquemment contrat avec des *start-up* et autres PME** car elle peut *in fine* y trouver intérêt à deux titres :

– en mettant les grands groupes en position de concurrence avec des PME plutôt qu'en position de chef de file monopolistique, comme tel est souvent le cas, **il n'est impossible que l'État obtienne de meilleures conditions tarifaires**, voire un produit adapté à ses besoins de façon plus souple. Tel a été le cas, par exemple, pour la *start-up* UserCube, dont les rapporteurs ont rencontré le fondateur, M. Christophe Grangeon, au « DGA Lab ». La DGA a trouvé intérêt à mettre cette *start-up* en concurrence avec Airbus pour la fourniture d'un système de référencement des personnels rattaché au système d'information des armées, dont c'est Airbus qui fournit une large part ;

– la DGA contribue ainsi à **vivifier l'écosystème des *start-up* innovantes**, non seulement par l'activité qu'elle leur offre, mais surtout parce que le référencement d'une société par la DGA est un gage de crédibilité pour nombre d'autres grands clients.

L'encadré ci-après présente les cas de quatre *start-up* avec lesquelles le ministère des Armées a pu passer contrat.

Quatre exemples de *start-up*
avec lesquelles le ministère des Armées a contractualisé directement

1./ UserCube, outil de gestion des mouvements de personnels, de leurs droits informatiques et des dotations en matériels

UserCube est un éditeur français de logiciels. Son fondateur, M. Christophe Grangeon, a précisé que sa clientèle est duale, comprenant des administrations publiques chargées de la cybersécurité, pour lesquelles le « *label français* » est important. Le cœur de métier de UserCube réside dans la gestion des collaborateurs et de leurs dotations en matériels et de leurs habilitations dans les systèmes d'information.

Pour UserCube, le système d'information des armées a représenté une clé d'entrée dans les marchés de la DGA. UserCube a en effet été sélectionné pour faire une présentation au DGA Lab en janvier 2014 pour la refonte de l'annuaire du ministère (AnnuDef) ; en décembre 2016, elle y est revenue pour une autre présentation et, dans un temps de convivialité suivant la session de travail, a pu approcher les représentants de la DGA ; celle-ci lui a ensuite commandé un produit « pilote » en mars 2017, au vu duquel elle a passé un marché, en cours de livraison à la date de la visite des rapporteurs. La « preuve de concept » a été faite à la DGA concernant le « socle projetable » de la gestion des identités des personnels engagés en opérations. La société a ainsi pu être référencée au catalogue de logiciels Ouranos sans passer par Airbus, fournisseur du socle projetable du SIA ; elle gère l'ensemble des habilitations d'accès au SIA pour les personnels engagés en OPEX.

Du point de vue financier, le ministère des Armées est un « petit » client. Mais le référencement par la DGA est un gage de crédibilité pour nombre de grands clients. Le DGA Lab a ainsi joué un rôle de déclencheur puis d'accélérateur de la relation de UserCube avec le ministère et, ce, à un coût commercial très modéré. Pour la DGA, l'intérêt tenait d'abord à connaître directement la *start-up*, pour mettre Airbus en position de concurrence.

2./ Virdys, programme de réalité virtuelle en 3D

Existant depuis 2012, la société possède les labels « jeune entreprise innovante » et « *French Tech* ». Sa suite logicielle permet de créer, d'animer et de diffuser des modélisations en 3D, maniables moyennant une formation de quatre jours, et ce sur un ordinateur classique et sans expertise spécifique.

Ses représentants ont souligné la difficulté qu'ils avaient eue à entrer en contact avec la DGA : « *il a fallu faire 9 000 km pour rencontrer les Français du Cercle de l'Arbalète au* Consumer Electronic Show *de Las Vegas en janvier 2016, ainsi que les représentants de Thales et d'Airbus qu'il était impossible d'approcher en France* ». Une session du « SIA Lab » en mars 2016 leur a permis de nouer des contacts avec la brigade de sapeurs-pompiers de Paris (BSPP) et la direction du renseignement militaire, qui a acquis des licences et les a renouvelées. Ensuite, lors d'une deuxième présentation en avril 2016, Virdys a pu prendre contact avec Sopra Steria pour la réalisation de modules de formation des militaires de l'opération Sentinelle aux règles d'engagement.

Les représentants de Virdys ont regretté les délais de paiement du ministère : huit mois pour un bon de commande, alors même que la société est référencée par l'UGAP. Pour eux, ces délais créent de trop grands besoins de fonds de roulement pour une PME. Leur correspondant habituel est l'adjudant-chef Delclos, informaticien-pompier affecté au bureau de l'ingénierie de la formation de la BSPP, chargé de la mise en œuvre d'un basculement des outils de formation vers la « ludopédagogie » (la formation par le « jeu sérieux »). Il a connu les produits de Virdys *via* le DGA Lab. Selon ses explications, la 3D correspond aux besoins de formation des jeunes : « *on a trois secondes pour attirer l'attention, vingt secondes pour les capter, et trois minutes pour démontrer ; c'est comme avec les autorités !* »

Pour eux, l'intérêt du « DGA Lab » tient à ce qu'une telle structure permet une rencontre directe entre les opérationnels et les *start-up*, à ce que le circuit de décision s'en trouve accéléré, et à la connaissance de l'écosystème d'innovation que permettent ces sessions. Ainsi, l'acquisition du premier « jeu sérieux » de la BSPP avait demandé deux ans de tests et deux ans de procédures, alors qu'avec Virdys, quelques mois ont suffi.

3./ Gladys, outils de travail collaboratif, de gestion de projets et d'innovation

Créée en 2013, la société Gladys est spécialisée dans les « digital workplaces *adaptées à la co-innovation* », l'idée de base consistant à créer un « *lieu numérique* » pour « *fédérer l'écosystème de l'innovation* ». Sa solution logicielle repose sur les piliers classiques de la collaboration : la communication (notamment par messagerie instantanée), la collaboration (partage de veille, lancement d'idées, etc.) ainsi que l'animation de projets et les piloter par des *portfolios* et des systèmes d'organisation, tels des outils de gestion de tâches. Le résultat est une sorte d'intranet amélioré, ou personnalisé, « *avec une large dimension de* design thinking », c'est-à-dire pensé à partir de l'usage.

La société Gladys a participé au DGA Lab en avril 2017, où elle a pu prendre contact avec le service du commissariat des armées qui lui a fait présenter des tests dès le mois de juin 2017. Selon les explications du commissaire en chef présent, l'outil donnait corps à une transformation digitale du service, pour « casser des silos », tout en étant conforme aux exigences de sécurité – un *cloud* sécurisé serait difficile à mettre en place sans grands investissements, aussi le commissariat a-t-il préféré continuer à maîtriser l'hébergement de ses données. La solution proposée par Gladys permet d'interconnecter des « briques » qu'Office 365 ou *Google* ne permettent pas de relier. Pour le SCA, le travail d'exploration fait par le « DGA Lab » a aussi permis de gagner du temps dans cette opération d'équipement.

4./ Golden Bees, société offrant des outils de ciblage intelligent de candidats par la publicité programmatique

GoldenBees produit une « plateforme de marketing RH », qui permet de démarcher des personnes à recruter *via* une publicité ; « *c'est la clé de jointure entre la gratuité du web et l'accès au bon candidat* ». Elle travaille actuellement sur tous types de profils : les soldats de 2e classe de l'armée de terre et les développeurs pour une grande banque française. La majorité des recruteurs passent en effet par des annonces et, suivant une logique passive, attendent des réponses. Or certains métiers connaissent parfois des pénuries de main-d'œuvre, et 30 % des entreprises disent rencontrer des difficultés de recrutement. D'où l'idée de diffuser des publicités ciblées, suivant les habitudes de navigation des candidats potentiels, de façon plus dynamique.

La société GoldenBees a présenté ses produits au DGA Lab en juin 2017, mais travaillait déjà à cette époque avec les armées de terre et de l'air en sous-traitance d'un grand groupe ; ainsi, le ministère des Armées ne connaissait tout simplement pas cette société.

La capitaine de l'armée de terre présente a expliqué qu'opérer 15 000 recrutements par an suppose 150 000 contacts, pour lesquels l'armée de terre a choisi de mettre un accent sur internet. Le coût s'élève à 40 euros au maximum par candidat sollicité, Golden Bees coûtant toutefois moins, dit-elle. Au total, le budget de communication de l'armée de terre consacré au recrutement s'élève à 12 millions d'euros, soit 400 euros par personnel recruté, ce qui est inférieur aux standards du secteur privé. L'armée de terre crée d'ailleurs sa *Data Management Platform* pour réduire ce coût par candidat ; dans cette optique, plus elle digitalise ses outils, plus elle peut faire d'économies.

À défaut de passer contrat directement avec des *start-up*, la DGA peut inclure dans les critères de ses appels d'offres une clause de recours à un vivier de

start-up et de PME et, dans la lignée des efforts entrepris avec le « Pacte défense PME », veiller à ce que les rapports de sous-traitance soient suffisamment équilibrés pour ne pas compromettre le développement des *start-up* et PME concernées. On relèvera d'ailleurs que le programme d'architecture de traitement et d'exploitation massive de l'information multi-source – concernant le *big data* – a fait l'objet d'un appel d'offres restreint auprès de cinq sociétés, l'appel d'offres mentionnant explicitement comme critère la mobilisation d'un tissu de PME et de *start-up*.

Pour les rapporteurs, une autre option mérite aussi d'être envisagée : la contractualisation avec un consortium de *start-up*. D'ailleurs, selon les explications de leurs interlocuteurs aux États-Unis, la charge administrative résultant du succès de la procédure précitée d'*Other Transaction Authority* – « *victime de son propre succès* » aux yeux des responsables d'IBM – a conduit le *Department of Defense* à promouvoir des **contrats collectifs, conclus avec un consortium de « petites » entreprises**, à charge pour le consortium de répartir entre ses membres l'activité commandée par le ministère. Les entreprises intéressées sont notamment celles identifiées par un service du Pentagone appelé ***Defense Innovation Unit experimental*** (DIUx).

De façon générale, le ministère des Armées a intérêt à contractualiser davantage avec des *start-up* et des PME, quitte à surmonter les difficultés administratives éventuelles et, surtout, les réticences prévisibles des grands groupes. D'ailleurs, même aux États-Unis, de telles réticences sont observées ; les responsables d'IBM ont même reconnu que les « grands » industriels, au-delà d'un discours convenu sur les vertus des *start-up*, y mettent en réalité des freins, car de tels dispositifs tendraient à les marginaliser.

c. Un équilibre à trouver dans le degré de centralisation du pilotage des acquisitions

Devant la commission, le chef d'état-major des armées a regretté une sorte de dépossession des chefs de corps et autres commandants d'unités en matière de soutiens et d'achats pour leurs régiments, bases ou navires. En effet, dans un premier temps, ce sont les chefs d'états-majors d'armées qui ont perdu une part de leurs responsabilités financières avec la loi organique relative aux lois de finances, qui a concentré les fonctions de « responsables de programmes » entre les mains des « grands subordonnés » du ministre de la Défense : le chef d'état-major des armées, le délégué général pour l'armement et le secrétaire général pour l'administration du ministère. Dans un second temps, c'est la création des bases de défense qui a privé les échelons inférieurs de commandement d'une large part de leurs compétences en matière d'achats. Aux yeux du général François Lecointre, ces réformes ont limité l'« agilité » des forces dans la gestion de leur équipement.

Ce constat a été pleinement partagé, pour ce qui concerne les équipements numériques, par l'officier général en charge de la transformation digitale des armées. Son adjoint, le colonel Pierre-Joseph Givre, a estimé que « *les dix*

dernières années ont été marquées par beaucoup de centralisation » des procédures de décision et donc de la gestion des crédits. Or, à Grenoble par exemple, où il a commandé un régiment, existent des viviers de *start-up* qu'il est difficile de connaître depuis Paris. D'ailleurs, il s'agirait de sommes limitées – quelques dizaines de milliers d'euros par unité –, et un effort de déconcentration est tout à fait admissible « *dans la mesure où un accompagnement (conseil juridique et contractuel notamment) est prévu et que l'on accepte l'échec* ».

Ainsi, sans remettre en cause l'architecture budgétaire ni l'organisation générale des soutiens, **davantage de subsidiarité est possible**, tant au niveau des régiments que des armées. Dans le cas de l'armée de terre, par exemple, il pourrait être utile – sans être excessivement coûteux – de confier aux chefs de corps un budget annuel destiné à l'expérimentation de nouveaux matériels, à l'acquisition d'équipements innovants ou à l'achat de matériels dont les forces pourraient faire un usage innovant en fonction de leur spécialité.

d. Pour répondre à ces différents enjeux, la réforme annoncée de « la 1516 » est très attendue

i. Une nécessaire réforme des textes réglementaires

Le rapport annexé au projet de loi de programmation militaire 2019–2025 annonce « *une réforme en profondeur de la gestion des programmes d'équipement* » aujourd'hui réglée par « la 1516 » précitée, en vue de raccourcir les cycles d'acquisition et de développer les capacités d'adaptation des armées aux évolutions technologiques.

Comme le rappelle le rapport récité du président Jean-Jacques Bridey, le processus actuel de conduite des opérations d'armement en France « *est reconnu pour assurer en moyenne une bonne maîtrise des coûts, des performances et des délais* ». D'ailleurs, « *les bons résultats à l'exportation témoignent également de sa valeur, puisque les matériels exportés sont en général dérivés de ceux développés pour répondre aux besoins des armées françaises, pour des montants bien inférieurs à ceux engagés, par exemple, aux États-Unis* ». Mais il reconnaît que tant le contexte actuel d'engagement des forces, où « *des réponses rapides à des besoins urgents sont de plus en plus recherchées, notamment face à l'évolution de la menace et à l'érosion de nos capacités* », que l'évolution des technologies civiles met aujourd'hui les opérations d'armement « *au défi d'exploiter au mieux les opportunités offertes et de gérer les risques associés – notamment l'obsolescence des composants intégrés aux systèmes d'arme* ».

Le président Jean-Jacques Bridey présente de la façon suivante les principales orientations de cette réforme :

– **renforcer la « *vision capacitaire* »** dans la conduite des investissements, consistant à définir les besoins d'abord en termes de capacités et à suivre, tout au long du déroulement des programmes, leurs développements sous l'angle de la réponse qu'ils apportent à ce besoin capacitaire ;

– **améliorer l'adéquation des équipements aux besoins des armées**, tant en termes de fonctionnalités, de coûts que de délais de mise à disposition ;

– renforcer la **maîtrise des coûts et des délais** des programmes et améliorer leur suivi ;

– conférer « ***plus d'agilité et d'adaptabilité*** » aux processus d'acquisition ;

– « ***mieux incorporer l'innovation issue de l'industrie et du secteur civil*** » et tirer le meilleur profit possible de la « révolution numérique » ;

– **intégrer *ab initio* dans les programmes le MCO des équipements**, leur coût d'utilisation et les infrastructures associées. Le délégué général pour l'armement a expliqué que ces contrats dits « globaux » intégreraient non seulement l'acquisition d'un matériel, mais également son MCO pour une période relativement longue, qui durerait généralement une dizaine d'années ;

– **favoriser les perspectives de coopération** et de mieux intégrer dans les projets les **perspectives d'exportation**.

Les rapporteurs soulignent l'importance, dans cette réforme, d'une différenciation des procédures en fonction des technologies présentes dans les différents programmes d'équipement, voire des enjeux financiers. En effet, si « la 1516 » a fait la preuve de son efficacité pour les « grands » programmes structurants, les programmes numériques (comme d'autres programmes de moindre envergure) méritent :

– des **procédures plus souples d'expression des besoins**, qu'il est souvent difficile d'énoncer de façon définitive pour des technologies nouvelles développées dans le secteur civil ;

– des **mécanismes de « boucle courte »** permettant d'accélérer l'équipement des forces ;

– des **spécifications** rédigées de façon à ne pas interdire l'intégration de nouvelles technologies en cours de développement, pour tenir compte des évolutions rapides des technologies numériques ;

– des **phases d'essais et de tests** plus efficaces et associant davantage les industriels et les armées ;

– la **prise en compte *ab initio* des besoins de développement incrémental et de MCO**, ce qui est particulièrement important, par nature, pour les systèmes informatiques, car leurs mises à jour ne constituent pas des opérations accessoires nécessitant par nature moins de crédits et moins de compétences que le développement initial du système.

ii. Une exploitation tout aussi nécessaire des marges de manœuvre légales dans le droit des marchés publics

Sans se livrer ici à une analyse très approfondie des facilités que permet le droit des marchés publics, les rapporteurs relèvent qu'aux yeux de nombre d'acteurs, les textes législatifs offrent au ministère des Armées des possibilités de contractualisation variées, dérogatoires aux procédures classiques, mais que ces possibilités ne sont pas exploitées aussi souvent qu'il serait pertinent.

À titre d'exemple de ces règles, on peut citer la **procédure de partenariat d'innovation** mise en œuvre par exemple pour le programme ARTEMIS précité, qui permet à la fois d'imposer aux grands industriels de constituer et d'associer un vivier de PME et de *start-up* et d'éviter de procéder à un appel d'offres une fois une solution technologique identifiée. Le rapport précité de notre collègue Cédric Villani souligne l'intérêt de cette procédure, comme le présente l'encadré ci-après.

La procédure de partenariat d'innovation

Cette procédure permet, dans une procédure de marchés, de couvrir le besoin de la phase de recherche amont et d'expérimentation jusqu'à la phase d'achat du produit opérationnel, sans avoir à remettre les acteurs en concurrence entre ces différentes phases. Ce point est l'une des difficultés majeures liées à l'exercice de l'exception de R&D : à l'issue des travaux, en cas de réussite et de volonté de passer à une étape opérationnelle, l'acheteur public a pour obligation de procéder à une remise en concurrence alors même que les expérimentations auraient été satisfaisantes et prometteuses.

Pour ne pas arranger la situation, il n'est pas rare qu'à l'issue de cette remise en concurrence, la solution déjà expérimentée n'emporte pas le marché de réalisation de la solution finale, souvent pour des raisons financières.

Source : Cédric Villani, mathématicien et député de l'Essonne, « Donner du sens à l'intelligence artificielle – Pour une stratégie nationale et européenne », rapport au Premier ministre, mars 2018.

La **procédure de dialogue compétitif** semble elle aussi bien adaptée à l'acquisition d'équipements innovants pour les armées, notamment, comme le souligne notre collègue Cédric Villani, pour des « *marchés complexes, pour lesquels l'acheteur public ne peut définir seul et à l'avance les moyens techniques qui vont répondre à son besoin, ou encore pour lesquels il n'est pas en mesure d'établir un montage juridique ou financier adapté* ». Cette procédure permet aux armées, directions et services de dialoguer avec les candidats au marché, afin de définir de façon itérative les conditions du marché.

Dans le même ordre d'idées, dans le programme d'études amont dit de *Man–Machine Teaming*, qui vise à appliquer certaines possibilités de l'intelligence artificielle à l'aéronautique de combat et dont l'animation a été confiée par la DGA à Dassault Aviation et Thales, la procédure retenue permettra de constituer un écosystème industriel et technologique innovant et souverain, intégrant des *start-up* et des PME.

Il ressort des travaux des rapporteurs que la frilosité des services du ministère chargés des achats et acquisitions dans l'exploitation de toutes les

marges de manœuvres permises par la législation en vigueur s'explique essentiellement par un **manque d'expertise juridique**, qui les conduit, par aversion au risque juridique, à s'en tenir aux procédures de droit commun.

Dans ces conditions, il s'agit moins de modifier les textes législatifs que les pratiques administratives. Pour ce faire, le ministère pourrait utilement mettre en œuvre des moyens d'appui en expertise juridique aux services compétents.

4. Des investissements à consentir pour stimuler la dynamique d'innovation

Structurer, consolider et stimuler un écosystème sectoriel de recherche et d'innovation autour du ministère des Armées suppose certains investissements techniques et, surtout, d'investir dans la formation et la mise à jour des compétences des professionnels du numérique comme de ses utilisateurs.

a. Des investissements dans des capacités de calcul

Le rapport précité de notre collègue Cédric Villani met en exergue, pour le cas de l'intelligence artificielle, un désavantage majeur de l'écosystème d'innovation français par rapport aux grands acteurs privés, notamment américains, en matière d'accès à des capacités de calcul. En effet, celles de nos concurrents sont « *quasi illimitées* », tandis que les capacités publiques offertes par le GENCI, comme indiqué *supra*, ne permettent de satisfaire la demande qu'à raison de la moitié ou du tiers des heures de calcul sollicitées.

Pourtant, les besoins de calcul intensif ont tendance à aller croissant avec l'approfondissement des recherches en intelligence artificielle, en *big data*, et avec le recours de plus en plus fréquent à la simulation dans tous les champs de la recherche. De surcroît, dans le champ de la R&D, les industriels y font de plus en plus appel, sans toujours posséder eux-mêmes leurs propres capacités de calcul – c'est-à-dire tant les supercalculateurs que leur environnement, notamment les personnels experts dans leur maniement.

Pour répondre à la demande croissante de moyens de calcul de notre écosystème d'innovation, notre collègue Cédric Villani préconise de créer un réseau d'« **instituts interdisciplinaires d'intelligence artificielle** » rassemblant l'ensemble des acteurs de l'innovation en la matière – chercheurs, étudiants et entreprises – et de **doter ces instituts d'outils de calcul** qui leur permettent de rivaliser avec les moyens des grands acteurs privés. Constatant que seule une partie limitée des recherches en intelligence artificielle nécessite des capacités de calcul intensif très poussées, il recommande de décliner l'offre de capacités de calcul de ces instituts en deux modalités :

– **un supercalculateur** conçu pour l'intelligence artificielle et dont l'usage serait réservé à la recherche française en intelligence artificielle (avec le cas échéant le soutien d'un industriel), précisant que les architectures informatiques

requises pour cette technologie « *diffèrent notablement de celles des supercalculateurs HPC classiques* » ;

– **un service de *cloud computing*** adapté à l'intelligence artificielle, qui serait négocié auprès d'un fournisseur de services européen et dont la recherche sera l'un des bénéficiaires.

Notre collègue Cédric Villani recommande de rendre l'accès à un tel supercalculateur spécialisé gratuit, au motif qu'une ouverture à des applications non « ouvertes » ne pourrait être que payante – sauf à constituer une aide d'État – et qu'un dispositif de tarification entraînerait « *en pratique une rigidité notable dans l'utilisation de l'outil* ».

L'intérêt d'une **politique favorisant l'accès de l'écosystème de recherche et d'innovation à des capacités de calcul** – supercalculateurs et services de *cloud computing* – se vérifie non seulement pour l'intelligence artificielle, mais pour bien d'autres développements technologiques dans le secteur de la défense, par exemple dès lors qu'ils ont recours à la simulation. Ainsi, par exemple, les rapporteurs ont pu constater que Naval Group utilise le calcul intensif, en se reposant sur ses moyens propres – ceux de ses sites de Nantes, de Cherbourg et de Lorient – pour les projets de teneur confidentielle, et sur les moyens du GENCI pour les recherches « ouvertes », c'est-à-dire celles dont les résultats sont publiés.

Mais si de « grands » industriels peuvent se doter de capacités de calcul, leur accès est moins aisé pour autres entreprises du secteur, alors même qu'elles ne sont pas les moins innovantes. En outre, mutualiser l'investissement en capacités de calcul au sein d'un même écosystème – ou d'une même « plateforme sectorielle » – en le confiant à un acteur dont tel est le métier permettrait d'en professionnaliser la gestion, c'est-à-dire de partager des compétences rares nécessaires à une exploitation optimale des capacités de calcul et une mise à jour régulière de ces équipements.

Aussi les rapporteurs jugent-ils utile d'étudier dans quelles conditions réglementaires **la puissance publique pourrait favoriser l'accès des industriels français partenaires de la défense à des capacités de calcul de pointe**, que ce soit en supercalculateurs ou en services de *cloud*.

b. Des investissements dans les ressources humaines

De façon peut-être paradoxale, dans la numérisation des armées, c'est peut-être par le facteur humain que le bât pourrait blesser et, ce, à deux égards. D'une part, l'écosystème d'innovation numérique a besoin d'un volume toujours croissant de ressources humaines bien formées, sans être toujours le plus compétitif des employeurs sur ce marché. D'autre part, l'appropriation des technologies numériques suppose un certain degré de compétences de l'ensemble de leurs utilisateurs.

i. Investir dans la formation d'une masse suffisante de **spécialistes du numérique**

- *Former les spécialistes dont les armées, la recherche et l'industrie ont besoin*

L'ensemble des autorités militaires et des responsables civils interrogés par les rapporteurs a fait état de préoccupantes difficultés de recrutement pour les postes appelant des compétences en matière numérique.

Tel est le cas, par exemple, de l'amiral François Moreau, qui a souligné le défi que constitue la fidélisation des « *compétences rares* » parmi les marins. Certes, le recours à des réservistes experts du numérique du fait de leur activité civile peut aider ; l'identification des marins les plus intéressés à titre personnel par ces technologies y contribue aussi. Mais l'effort d'attractivité et de fidélisation restant à accomplir est très conséquent. De même, le général Barrera a cité plusieurs spécialités pour lesquelles le manque de candidats est particulièrement net dans l'armée de terre : ***designers*, cogniticiens, *data scientists,* et spécialistes du *cloud*, des interfaces API ou des technologies de *blockchain***.

Ce constat, qui est le même dans les trois armées, est fait également par le vice-amiral d'escadre Arnaud Coustillière. Pour lui, les difficultés de recrutement de la « chaîne » des systèmes d'information et de communication tiennent aux réticences que suscite parfois encore le caractère militaire de l'institution, au manque d'attractivité des grilles de rémunération, au nombre restreint de personnels formés chaque année, ainsi qu'à la politique de déflation des effectifs des années précédente, qui a vu, par un regrettable effet d'aubaine, les personnels disposants de compétences concernées se porter volontaires parmi les premiers pour quitter l'institution et bénéficier des aides au départ, alors qu'ils trouvent plus facilement que les autres à se reclasser dans le secteur civil. La difficulté porte particulièrement sur les sous-officiers. En effet, pour les officiers, les armées peuvent recruter des officiers sous contrat pour une mission relativement courte, d'autant plus aisément que le temps de formation militaire de ces personnels est souvent court. Les armées, directions et services ont mis en œuvre des plans d'action, accroissant le recours à des contractuels, et l'atteinte des objectifs fixés devra faire l'objet d'une vigilance soutenue.

Les dirigeants du GENCI ont également signalé un **déficit de spécialistes français du calcul intensif**, notamment pour les compétences de codage des logiciels intermédiaires, manque « *qui ira en s'aggravant* ». Manquent aussi des « **bi-scientists** », c'est-à-dire des scientifiques d'une discipline particulière qui, sans nécessairement pouvoir coder, sont capables d'intégrer finement les capacités de supercalcul dans leurs programmes de recherches, notamment en définissant les métadonnées nécessaires – dans le secteur de la santé, par exemple, il s'agit de scientifiques capables à la fois de comprendre la biochimie et le calcul intensif. Ces compétences seront particulièrement critiques pour les applications d'aide à la

décision, qui reposent sur les sciences humaines et sociales. En outre, « *plus les compétences sont rares, plus elles sont chères…* »

Notre collègue Cédric Villani fait le même constat pour les spécialistes de l'intelligence artificielle, comme le montre l'encadré ci-après. Il propose « *un objectif clair* » : « ***à horizon trois ans, multiplier par trois le nombre de personnes formées*** *en intelligence artificielle en France* », à la fois en orientant vers ces spécialités l'offre existante de formation et en créant de nouveaux cursus, à l'ensemble des niveaux de qualification de l'enseignement supérieur.

Une pénurie d'ingénieurs formés à l'intelligence artificielle

Déjà en 2011, un rapport de McKinsey Global Institute déclarait qu'on manquerait de 190 000 *data scientists* en 2018, ainsi que de 1,5 million de managers et d'analystes capables tout simplement de comprendre les enjeux et de prendre des décisions dans le contexte de l'intelligence artificielle.

L'étude de Burning Glass Technologies, BHEF et IBM parue début 2017, quant à elle, prédit que le nombre d'emplois dans le monde pour des *data scientists* et *data analysts* va augmenter de 28 % dans les cinq prochaines années, pour atteindre 2 720 000, et que 39 % de ces emplois demandent une qualification niveau master ou doctorat.

Enfin, en décembre 2017, selon une étude compilée par le *Tencent Research Institute*, il n'y a aujourd'hui que 300 000 « chercheurs et praticiens de l'intelligence artificielle » dans le monde, alors que la demande du marché se chiffrerait en millions (même si les méthodes utilisées pour arriver à ces résultats ne sont pas détaillées). Le goulot d'étranglement, pour *Tencent*, serait précisément la formation. Incidemment, cette étude cite les États-Unis, la Chine, le Japon et la Grande-Bretagne comme les pays les mieux placés dans la course à l'IA, avec mentions spéciales pour le Canada et Israël, en particulier en matière de formation. La France n'est pas citée.

Il faut donc à la fois former davantage d'ingénieurs et de techniciens dans les spécialités du numérique.

Source : Cédric Villani, mathématicien et député de l'Essonne, « Donner du sens à l'intelligence artificielle – Pour une stratégie nationale et européenne », rapport au Premier ministre, mars 2018.

- *Fidéliser les spécialistes du numérique dans les armées, la recherche et l'industrie françaises*

Augmenter la taille des viviers de spécialistes ne produira son plein effet que si est jugulée ce que notre collègue Cédric Villani appelle **« *l'hémorragie* » des ingénieurs et chercheurs français** : « *chaque semaine des chercheurs sont recrutés par les entreprises privées et souvent étrangères et quittent les laboratoires publics* ». Ces difficultés de recrutement pourraient s'accroître pour l'ensemble des acteurs de l'écosystème français, à mesure que les grands acteurs américains qui recrutent volontiers des Français, par exemple en Californie, en viennent à ouvrir des centres de recherche en France même, comme l'ont récemment annoncé *Facebook* et *Google*.

Le manque d'attractivité de la recherche publique française s'analyse bien entendu en termes de rémunération, dont notre collègue Cédric Villani recommande un effort de revalorisation très conséquent. De même, M. Axel

Legay, directeur de la chaire « cybersécurité sur l'analyse de la menace » de l'INRIA, a indiqué que les partenaires industriels de son laboratoire ne manquent pas de faire à ses chercheurs des offres particulièrement attractives : « *un chef d'équipe de recherche, fonctionnaire qui a dix ans d'ancienneté et une solide expérience par ailleurs, gagne, après taxes et impôts, la même chose qu'un étudiant en thèse en Belgique… tandis que les salaires offerts par des sociétés américaines, pour les mêmes compétences, vont du double au triple* ». Le manque d'attractivité a aussi une dimension statutaire : M. Axel Legay a indiqué que son laboratoire, qui travaille à la fois avec la DGA et avec CISCO, emploie des spécialistes des *malwares* parmi les plus compétents au monde, mais que légalement, il ne peut pas les recruter en contrat à durée indéterminée – ce qui, d'ailleurs, ne coûterait pas davantage. Concernant les personnels régis par le statut de la fonction publique, les grands acteurs américains offrent des possibilités de progression de carrière plus attractives que ne le font les règles d'avancement.

ii. Développer une **culture du numérique**

Comme l'a constaté M. Antoine Petit, « *l'inculture numérique est générale* » : elle commence dès la formation initiale des Français – pas seulement des militaires – et peut toucher même des titulaires de hautes responsabilités. En conséquence, **un effort d'acculturation générale au numérique est particulièrement nécessaire dans les armées** à plusieurs égards.

D'abord, la bonne utilisation de systèmes d'armes numérisés suppose, de la part des militaires de tout grade, une certaine culture numérique. Schématiquement, toute innovation suppose une formation, et certains suggèrent que des critères de « cyber-hygiène » soient intégrés aux conditions d'aptitude des militaires, quel que soit leur grade.

Surtout, la diffusion de la culture numérique au sein du commandement opérationnel peut constituer une condition de confiance dans les technologies numériques avancées. Comme l'a fait valoir le général Bernard Barrera pour le cas de l'intelligence artificielle appliquée aux systèmes d'aide au commandement, l'intelligence artificielle devra être déployée au niveau tactique ou à l'échelon opératif et « ***ses préconisations ne seront suivies par le général sur le terrain que si son état-major est "armé" par des*** **data scientists** ***capables d'expliquer et de justifier les recommandations faites par la machine*** », dès lors qu'est en jeu la responsabilité d'engager des hommes au feu. Une certaine expertise doit donc irriguer l'ensemble de la chaîne de commandement.

III. LA TRANSFORMATION NUMÉRIQUE NE DISPENSE NI DE DISPOSITIFS DE RÉSILIENCE NI D'APTITUDES À OPÉRER « EN MODE DÉGRADÉ »

Pour nos armées, la numérisation offre certes des opportunités considérables, mais elle ne doit être vue ni comme une fin en soi, ni comme une sorte de magie. Que l'on ne se leurre pas : la numérisation ne signifie pas la fin de la guerre. Sur le plan opérationnel, elle crée de nouvelles vulnérabilités que nos armées doivent pouvoir parer en leur sein comme exploiter chez l'adversaire.

A. LA NUMÉRISATION DES ARMÉES NE REND QUE PLUS NÉCESSAIRES DES MOYENS EFFICACES DE CYBERDÉFENSE ET DE RÉSILIENCE

Approfondir la numérisation des armées, c'est accroître leur **surface d'exposition numérique et, partant, leur vulnérabilité** aux attaques dans le champ numérique. Mais la vulnérabilité numérique revêt deux aspects indissociables : d'une part, elle appelle pour nos forces des efforts accrus de cyberdéfense et, d'autre part, elle offre chez l'adversaire « numérisé » de nouvelles prises qu'il convient d'exploiter à tous les échelons de la conduite des opérations, y compris au niveau tactique.

1. La résilience des infrastructures numériques dans leur ensemble constitue un point d'attention

En même temps que la mission d'information dont les rapporteurs présentent ici les conclusions, la commission a créé une mission d'information sur la cyberdéfense, dont les conclusions seront assurément complémentaires de celles des rapporteurs. Ceux-ci ne traiteront donc pas les questions de cyberdéfense à proprement parler ; mais loin d'empiéter sur le champ d'investigation de cette autre mission d'information, ils tiennent à souligner combien la numérisation des armées risque de créer une porosité entre la protection des infrastructures civiles et celle des infrastructures militaires. Il importe en effet que les armées demeurent capables de fonctionner « en mode dégradé ».

Comme l'a fait valoir un haut responsable d'un service de renseignement, « *la sécurité des équipements numériques n'est pas spontanément une priorité pour les développeurs* » du fait de trois caractéristiques de l'industrie numérique :

– l'essentiel des développements technologiques est tiré par **l'industrie des loisirs**, comme le jeu ou le cinéma, même pas par les usages professionnels, fussent-ils civils ;

– les **technologies sont désormais monopolistiques** : « *de l'avion à la centrale numérique en passant par les jeux, on retrouve les mêmes puces, les mêmes protocoles IP, les mêmes systèmes de routeurs* » ;

– enfin, « ***rien n'est normé*** *dans le monde numérique* » : ainsi, par exemple, Skype n'a jamais été configuré de façon à « router » en priorité les appels d'urgence.

a. L'impératif de résilience des réseaux du ministère des Armées présente la spécificité de s'appliquer à un ensemble de systèmes très divers

i. Des réseaux hétérogènes

Pour M. Guillaume Poupard, directeur général de l'ANSSI, l'état de nos défenses est « *en demi-teinte* » car si beaucoup d'efforts sont faits, il faut néanmoins gérer des **réseaux hérités du passé**. Sécuriser un réseau moderne n'est pas complexe ; mais les réseaux du ministère des Armées sont hérités de réseaux anciens, conçus « en silos » à une époque où la résilience en cas d'attaques cybernétique ne constituait pas une préoccupation prioritaire.

Aussi le directeur général de l'ANSSI a-t-il dit avoir **confiance à la fois dans l'avenir** – car les programmes actuels intègrent bien la cybersécurité – et **dans le passé** – car nos « vieilles » plateformes, peu numérisées, sont peu vulnérables. Il a cependant estimé que **l'inquiétude peut porter davantage sur les programmes assez récents** pour être numérisés mais assez anciens pour n'être pas suffisamment protégés.

M. Patrick Hebrard, responsable de l'innovation et de la recherche cyber de Naval Group, ancien titulaire de la chaire « cyberdéfense des systèmes navals » de l'École navale, a expliqué qu'au moins pour ce qui concerne les bateaux, cohabitent **trois familles de systèmes** numériques :

– des systèmes fonctionnant « en temps différé », qui opèrent dans la seconde, à l'image des systèmes d'exploitation des ordinateurs commerciaux ;

– des systèmes fonctionnant « en temps réel » à la milliseconde ;

– des systèmes fonctionnant « en temps industriel » à la microseconde.

La cohabitation de différents systèmes sur une seule plateforme ne rend que plus compliquée la défense de celle-ci contre les attaques cyber. L'outil de combat repose en effet sur une multiplicité d'entités et de systèmes qui interagissent avec hommes, d'où une multiplicité de « maillons » qui augmentent la vulnérabilité de la chaîne dans son ensemble. Selon l'expression de M. Paul Théron, titulaire de la chaire Cyb'Air de l'armée de l'air, « *un chaos inextricable d'objets connectés* » est par nature vulnérable aux attaques cybernétiques.

ii. Des menaces qui peuvent rester « dormantes » un certain temps

M. Patrick Hebrard a indiqué qu'à ses yeux, la cybermenace « en temps réel » fait l'objet d'une pleine prise de conscience, mais que tel n'est pas toujours le cas de **menaces dormantes** – qu'il s'agisse de *malwares* ou de « bombes

logiques » – qui pourraient être activées par un signal extérieur. Ainsi, un réseau ancien qui est en apparence sûr peut comporter une menace « à retardement ».

M. Paul Théron a ajouté que les cybermenaces évoluent elles aussi, et que les *malwares* deviendraient vraisemblablement **autonomes et intelligents** : ils analyseront leur environnement, en trouveront les failles, créeront un plan d'attaque et l'exécuteront et ce, en s'adaptant aux défenses voire en masquant leurs traces. Il estime que cette menace est à prendre au sérieux, et qu'il faudrait de longs travaux de recherches pour élaborer des contre-mesures que l'on appelle « systèmes multi-agents de cyberdéfense ».

b. La connexion à des réseaux ouverts accentue la vulnérabilité des systèmes d'information du ministère des Armées

En dépit de la spécificité des missions de la défense, les systèmes d'information des forces armées sont parfois soit connectés aux réseaux de leurs fournisseurs, soit dépendants de réseaux civils.

i. La question de la résilience des systèmes d'information des soutiens et des vulnérabilités qu'elle crée pour les forces

- *Les opérations de MCO, occasion de connexion des réseaux et* ipso facto *de vulnérabilités*

M. Guillaume Poupard a fait observer que les systèmes d'information présents au sein d'un système d'armes ou gravitant autour sont nombreux, cloisonnés ou non. Le ministère des Armées bénéficie des dispositions légales relatives à la classification : tous les systèmes d'information des armements étant par nature dans la sphère classifiée, ils ne sont à peu près jamais reliés aux réseaux ouverts ; **tel n'est pas le cas, en revanche, des autres systèmes d'information**, comme par exemple les systèmes d'information de la propulsion d'un bateau.

M. Gérard de Boisboissel a ajouté que l'externalisation croissante des systèmes d'information et de la maintenance de ces systèmes conduit à une **multiplication des interconnexions avec les industriels ou des organismes externes**, favorisant l'apparition de nouvelles vulnérabilités si ces systèmes d'information sont raccordés à internet, comme tel pourrait être le cas, par exemple, des systèmes d'information d'opérateurs de tâches logistiques. La vulnérabilité va en effet croissant avec la numérisation croissante du MCO des systèmes d'armes. Pour le directeur général de l'ANSSI, « *c'est le sens de l'histoire : hier, un bateau était livré avec sa boîte à outils, et les marins réparaient tout eux-mêmes ; puis, au gré de la modernisation des équipements et de la déflation des effectifs,* ***le MCO a été externalisé et numérisé*** » : schématiquement, un bateau qui connaît une avarie regagne un port où des maintenanciers de Naval Group viennent et se connectent au bateau. Et demain, il n'est pas impossible que l'on répare les systèmes d'armes à distance.

- *Les systèmes d'information d'administration et de gestion, des réseaux essentiels mais moins protégés*

Par ailleurs, les rapporteurs se sont attachés à étudier quel est le degré de résilience de la chaîne des soutiens en cas d'indisponibilité des SIAG. Selon le secrétaire général adjoint pour l'administration du ministère des Armées, si ceux-ci étaient hors service, le ministère mettrait en place un plan d'urgence, comme il l'a fait par exemple pour traiter les dysfonctionnements du système Louvois. En outre, **dans le développement de chaque système d'information, la sensibilité de chaque système est évaluée**, et pour les systèmes reconnus comme « essentiels », des mesures de sécurité sont prises.

Par ailleurs, **le ministère des Armées conserve des compétences**, ne serait-ce que pour paramétrer les systèmes d'information et les alimenter en données. Depuis 2014, le SGA identifie des **métiers administratifs cruciaux** ; chaque direction ou service est ainsi responsable de l'entretien des familles professionnelles rares ou cruciales. En outre, l'homogénéisation et la professionnalisation des services ont enrichi les compétences des « métiers » du SGA. Enfin, les expériences d'autres acteurs français en cas de cyberattaque montrent que les systèmes visés sont généralement les moins protégés : il en est ressorti une **prise de conscience**. En tout état de cause, le ministère des Armées **protège les données**, condition *sine qua non* d'un redémarrage de ses systèmes d'information après un incident.

Pour autant, **le ministère n'a pas de grand plan de continuité de service en « mode dégradé » de ses systèmes d'information** ; il a des plans de continuité de l'activité, par exemple pour les cas d'inondations. Mais « *pour les SIAG, le sujet de la résilience est encore devant nous pour une large partie* ». Face aux dysfonctionnements du système Louvois, le ministère a fait appel à de « jeunes » retraités pour venir pallier, par des reprises manuelles, les erreurs du système, mais rien ne dit que cela soit possible pour tous les systèmes dans l'avenir.

ii. La dépendance du ministère des Armées aux réseaux civils

Certains systèmes opérés par les forces reposent sur des infrastructures de réseaux civils, celles d'opérateurs d'importance vitale, dont la résilience en cas de cyberattaque constitue un impératif pour le bon fonctionnement de certaines activités militaires.

Ainsi, même si cet exemple ne touche pas directement les armées, les rapporteurs ont étudié le cas du système Neogend, outil numérique permettant aux gendarmes d'effectuer la plupart de leurs tâches quotidiennes. En la matière, un des freins à la numérisation des procédures de la gendarmerie nationale peut tenir aux **problèmes de couverture numérique du territoire national**. Si la gendarmerie n'a pas de pouvoir d'injonction sur les opérateurs pour améliorer la couverture du territoire, elle entretient un dialogue avec eux et plaide en faveur de l'extension des zones dites « blanches » dans lesquelles les opérateurs peuvent

s'associer pour couvrir le territoire. En outre, elle plaide en faveur d'une couverture de zones plus larges que les seuls centres-bourgs des zones rurales.

Il importerait donc que les infrastructures civiles critiques même pour le fonctionnement des forces intègrent les contraintes des forces de sécurité intérieure et des armées. Avec les professeurs Steeve Bloor et Paul Gillespie, de l'*Eisenhower School*, les rapporteurs ont pu étudier le cas de la cinquième génération de standards pour la téléphonie mobile (dits « la 5G »). Les enjeux de résilience et de sécurité des télécommunications, auxquels sont confrontés tous les pays, incitent à définir des standards robustes et relativement détaillés, pour conduire par avance les industriels à s'adapter à des infrastructures répondant à des spécifications tenant compte des impératifs de la sécurité nationale. Mais un équilibre subtil est à trouver en la matière entre, d'une part, les impératifs de sécurité, qui peuvent étouffer l'innovation et, d'autre part, l'intérêt de l'innovation technologique, qui suppose une large autonomie du secteur privé.

iii. Les vulnérabilités potentielles liées aux composants informatiques « non-souverains »

Comme l'a expliqué le vice-amiral d'escadre Arnaud Coustillière, le postulat de base en matière de sécurité numérique est qu'**aucun constituant des systèmes d'information ne peut être considéré comme de confiance**, de la puce à la brique logiciel en passant par l'alimentation ou les cartes physiques, « *et que dire des antivirus…* ». Ce postulat est aussi que « *tout cela peut être piégé* », il faut donc mettre en place « *des défenses en profondeur, des surveillances internes, du chiffrement, de la "séparation / ségrégation" et des points de mesures via des sondes et des bases de connaissance régaliennes* ».

Faute d'une industrie française forte en matière de composants informatiques, « *il faut être capable de produire et déployer très rapidement des correctifs et des mises à jour* » quand une vulnérabilité ou une attaque est repérée. Il faut aussi être capable de « stresser » ces briques logicielles – c'est-à-dire les faire tourner à plein régime pour tester leur fiabilité.

iv. Résilience et « réversibilité numérique »

Dans l'idéal, l'impératif de résilience des systèmes d'information que commande l'état de ces vulnérabilités devrait conduire à ce que la numérisation des systèmes soit réversible.

Toutefois, **une réversibilité totale de la numérisation des systèmes n'est pas réaliste**. Comme l'on dit les responsables de la R&D de Naval Group, la réversibilité totale de la numérisation des systèmes d'armes n'est plus nécessairement recherchée, car de même qu'« *on ne fournit plus de manivelle pour faire démarrer les voitures* », il faut « *abandonner certaines fonctions anciennes quand on a suffisamment confiance dans les technologies plus récentes* ». Tel est d'ailleurs l'enjeu du dialogue entre le fournisseur d'un système

d'information et les « opérationnels » parmi lesquels certains « *ont tendance à n'avoir confiance que dans les technologies analogiques* ».

2. La vulnérabilité des forces s'accroît avec leur surface d'exposition numérique

Les vulnérabilités des armées aux cyberattaques vont croissant avec leur « **surface d'exposition numérique** », c'est-à-dire leur dépendance des infrastructures de réseau. Cette surface s'est considérablement étendue à mesure qu'ont été numérisés les systèmes d'armes, l'ensemble des procédures d'administration et de gestion des armées, ainsi que les infrastructures civiles constituant l'environnement des forces. De plus, comme l'a souligné le directeur général de l'ANSSI, **le temps est dépassé où l'on pouvait penser le numérique comme « un plus »**, dont on bénéficie mais dont on pourrait s'abstraire pour revenir à un « mode dégradé » complet.

Cet état de fait crée pour nos armées à la fois **un risque – être attaqué *via* le numérique – et une chance : attaquer l'adversaire en exploitant ses vulnérabilités numériques**. Sans empiéter sur le champ de compétence de la mission d'information précitée sur la cyberdéfense, les rapporteurs soulignent qu'en la matière, l'avers comme le revers de la médaille appellent une attention soutenue à la cyberdéfense dès la conception des programmes d'armement.

a. La numérisation de nos armées suppose un effort de lutte cybernétique défensive qui commence dès la conception des équipements

Dans des armées largement numérisées, l'effort de cybersécurité doit porter sur l'ensemble des éléments numériques (faute de quoi les systèmes d'information les moins sécurisés, car les moins « opérationnels », peuvent être le talon d'Achille d'une force), et gagne à être pris en compte dès la conception de l'architecture des équipements numériques.

i. La prise en compte de la cybersécurité doit commencer dès la conception de l'architecture d'un équipement

Selon les explications des autorités techniques compétentes, **dans la protection de nos systèmes, beaucoup tiennent à leur architecture**. C'est ainsi dès la conception de l'architecture du système d'information d'un équipement que sa cybersécurité doit être prise en compte.

Cet impératif est particulièrement prégnant pour les équipements de forces isolées sur un théâtre d'opération. À cet égard, les plateformes maritimes constituent aux yeux de certains experts « *des cibles de choix* » pour les cyberattaques, car les navires n'embarquent que peu de techniciens – à plus forte raison avec la tendance observée à la réduction des effectifs des équipages –, alors que parer une attaque suppose des opérations compliquées d'investigation et des remèdes souvent eux aussi complexes. C'est d'ailleurs ce qui explique la mise sur pied de groupements d'intervention rapide (GIR) par la marine nationale : le

centre technique de lutte informatique défensive (CTLIC) peut dépêcher des équipes quand une attaque ne peut pas être contrée par l'équipage et que les systèmes attaqués ne sont pas intégralement télé opérables.

M. Patrick Radja, responsable technique de la cybersécurité de Naval Group, a expliqué comment **la menace cybernétique est prise en compte dans l'architecture informatique des bateaux dès la conception de ceux-ci**, par des moyens d'isolement des différents équipements, des redondances fonctionnelles (utiles également en cas de panne d'électricité) et des systèmes de lutte informatique défensive.

Le déplacement à Ollioules a également permis aux rapporteurs de se faire présenter les travaux du *Naval Cyber Laboratory* de Naval Group. Pour garantir que des bateaux de plus en plus numérisés soient numériquement sûrs, la protection des plateformes contre les cyberattaques est prise en compte dès la conception des navires. Elle suppose de maîtriser la sûreté numérique de l'ensemble de la *supply chain*, car **la principale menace à prendre en compte, pour les ingénieurs de Naval Group, tient à la pose d'une « bombe logique » à l'occasion d'une opération industrielle**. La cybersécurité passe donc par des dispositifs de détection, de compréhension et de réponse aux attaques informatiques dont l'encadré ci-après présente le fonctionnement.

Le *Cyber Management System* d'un navire moderne

Une démonstration de lutte informatique défensive a été faite aux rapporteurs chez Naval Group à partir d'un tableau de suivi de la cybersécurité (*Cyber Management System*, CyMS). Ce tableau – conçu pour être aussi lisible que possible par un marin qui n'est pas spécialiste – présente de façon synthétique l'ensemble des incidents repérés ; l'équipage peut envoyer des données à terre, où l'on peut proposer des solutions de traitement des défaillances pour restaurer les fonctions, toujours soumises à l'accord du commandant.

Le CyMS est lui-même très protégé, et demeure en tout état de cause déconnecté des systèmes d'information opérationnels : une seule et même attaque ne peut pas détruire les deux systèmes.

Naval Group souligne la nouveauté de ces équipements. La menace cybernétique n'a en effet été pleinement prise en compte qu'avec le programme de frégate de taille intermédiaire, postérieur au programme de frégate multi-missions.

L'importance d'une prise en compte de la cybersécurité dès la conception de l'architecture d'un système vaut bien entendu pour toutes les plateformes, dans tous les milieux d'opération. En matière de plateformes aériennes, par exemple, M. Éric Trappier a souligné qu'en matière de sécurité, « ***tout tient à l'architecte,*** *qui pense un système avec ses protections* ».

ii. L'effort de cybersécurité doit porter aussi sur les cibles « molles », talon d'Achille d'un système d'armes

Mme Frederick Douzet, titulaire de la Chaire Castex de cyberstratégie de l'IHEDN, a fait observer que l'attaque menée avec le logiciel *Wannacry* procédait

d'une **logique d'attaque de cibles dites « molles »** : elle a visé – et frappé – des cibles moins défendues que les systèmes d'armes. S'agissant des cibles militaires, une opération de *hacking* terroriste supposerait un important travail de renseignement – ne serait-ce que pour avoir les plans des systèmes informatiques des armements, qui sont difficilement accessibles sans complicité chez l'industriel –, pour un effet incertain, en tout état de cause moins spectaculaire et moins terrifiant qu'une tuerie de masse. Il faudrait en outre connaître les contextes d'emploi des armes et l'état des connexions opérationnelles, ainsi que trouver un point d'entrée dans les systèmes.

L'effort de cybersécurité doit donc être général, au-delà même du périmètre du ministère des Armées. Un tel effort ne semble d'ailleurs pas excessivement coûteux. En effet, selon le directeur général de l'ANSSI, **la sécurisation des systèmes d'information revient en moyenne à 5 % de leur coût** : « *c'est cher, mais pas hors de portée* ».

b. La numérisation des forces adverses ouvre la voie à des possibilités de lutte cybernétique offensive, y compris au niveau tactique

Le recours croissant de nos adversaires – même non-étatiques – à des moyens numériques les expose aux mêmes types de vulnérabilités que nos forces. Comme l'a indiqué le directeur général de l'ANSSI, le **volet offensif** de nos capacités de lutte cybernétique, opéré par la DGSE en lien étroit avec l'état-major des armées, passe par des attaques de nature subtiles, en appui aux opérations : « *c'est une arme d'emploi avec une plus-value opérationnelle certaine* ». L'avantage de ces capacités offensives est d'être potentiellement ciblées, et souvent réversibles.

Si la lutte cybernétique offensive est pour l'heure très centralisée au niveau stratégique, la numérisation croissante du combat peut conduire à étudier des possibilités de mettre en place des dispositifs cybernétiques offensifs sur certaines plateformes afin de les mettre en œuvre depuis le niveau tactique.

D'ailleurs, le contre-amiral François Moreau, sous-chef d'état-major chargé des plans et des programmes de l'état-major de la marine nationale, a indiqué que la marine ne s'interdit pas de réfléchir aux **moyens de vaincre sans même utiliser d'effet « cinétique »** – c'est-à-dire d'armes classiques, ayant un effet « physique ». Parmi ces moyens, l'amiral François Moreau a cité, à titre d'exemple, la lutte informatique offensive et les armements électromagnétiques qui pourraient être à même de neutraliser les systèmes numériques de l'adversaire. Pour lui, **l'avenir est certainement à un emploi plus tactique des moyens d'action cybernétiques, mis en œuvre de façon plus décentralisée**. Ainsi, par exemple, un commandant de navire pourrait utilement disposer, en plus de ses moyens cinétiques, de moyens cybernétiques offensifs.

Ces moyens sont d'ailleurs moins propres à un milieu que ne le sont les moyens « cinétiques ». On pourrait ainsi imaginer, dans la lignée des moyens de

guerre électronique d'ores et déjà mis en œuvre, **l'incrémentation de moyens cybernétiques au système de combat SCORPION**, prévu pour l'étape 2 de cette opération, se traduise par des moyens offensifs disposés directement sur certaines plateformes de la « bulle SCORPION ».

B. MÊME NUMÉRISÉES, LES ARMÉES DEVRONT CONTINUER À ÊTRE CAPABLES D'OPÉRER « EN MODE DÉGRADÉ »

Dans la numérisation des systèmes d'armes, on l'a dit, une réversibilité totale est une illusion ; mais une irréversibilité totale serait un grand risque. Aux yeux des rapporteurs, il importe que les équipements, même numérisés, puissent encore fonctionner « en mode dégradé » et ce, pour deux ordres de raisons. D'une part, il est difficile de garantir que leurs moyens de cyberdéfense ne soient jamais dépassés par des moyens de cyberattaque adverses dans les décennies à venir. D'autre part, de façon plus générale, la prudence et les retours d'expérience des opérations occidentales récentes tendent à montrer que si l'« hypertechnologie » permet de remporter des batailles, elle ne suffit pas à gagner les guerres.

1. Opérer « en mode dégradé » pour gagner la bataille, face aux menaces pesant sur nos équipements numériques

Comme l'a expliqué M. Axel Legay, il est vraisemblable que **les systèmes défensifs auront la plupart du temps du retard sur l'évolution des systèmes offensifs**. M. Patrick Hebrard a précisé que ce décalage est d'autant plus vraisemblable que la conception d'un logiciel « attaquant » est structurellement plus aisée que celle d'un logiciel de défense ; en effet, l'attaquant « *a pour seul but de "faire mal", peu importe de comprendre très précisément comment* » : il est d'autant plus difficile de s'en protéger qu'un dispositif défensif doit préserver son environnement. Pour lui, c'est ce qui fait la plus-value de l'analyse comportementale dans l'élaboration de défenses cyber : juger si un lien, une connexion, un comportement même conforme aux règles est de nature « normale » sert à repérer les comportements suspects et, le cas échéant, à alerter.

Mais rien ne garantit que toute attaque cybernétique, même décelée, pourra être réparée dans des délais convenables. Dès lors, **il importe que les armées demeurent capables d'opérer en « mode dégradé », c'est-à-dire en se passant de certaines fonctions numériques**. Pour certains observateurs, « *les Américains s'en sont rendu compte en Ukraine : les Russes sont à jour en matière technologique, et les postes de commandement redeviennent un point de vulnérabilité* ». Le développement des équipements numériques est donc utile, mais il faut **conserver de la « rusticité »**, ce qui suppose à la fois des matériels et une formation appropriés.

a. Des matériels capables de fonctionner « en mode dégradé »

Pour le cas de l'armée de terre, par exemple, le général Bernard Barrera a assuré les rapporteurs qu'elle est consciente de son intérêt à pouvoir toujours

opérer en « mode dégradé », faisant valoir que « *cela fait partie de la culture opérationnelle fondamentale de l'armée de terre* ». Il serait en effet dangereux que les soldats ne sachent pas opérer sans équipements numériques de tir, de pilotage ou de confort ; en la matière, « *la résistance physique et la force morale comptent* ». Le général Bernard Barrera a raconté qu'ainsi, les systèmes d'information ne fonctionnaient pas lorsque la colonne Serval, débarquée à Bamako depuis quatre jours, a reçu l'ordre de marcher sur Bamako ; « *il a donc fallu acheter des téléphones portables et des puces sur le marché de Bamako pour que la colonne se repère, alors que les drones fournissaient une capacité de vision assez satisfaisante à Paris* ».

Les experts de l'état-major de l'armée de terre ont aussi souligné qu'une certaine **redondance des moyens de transmission** est utile pour conserver une capacité de commandement suffisante, même en « mode dégradé ». Il en va ainsi, par exemple, des équipements radios « classiques », qui permettent par exemple à un militaire de Sentinelle d'utiliser la radio de la police en cas de défaillance des systèmes de communication plus performants, . Autre illustration de cette idée, le retour d'expérience de l'opération Serval met en lumière l'utilité de moyens de communication satellitaire utilisables en mouvement (« *SATCOM on the move* ») en complément des moyens existants (les radios à haute et très haute fréquence).

Le potentiel de résilience et les capacités de fonctionnement en « mode dégradé » de nos équipements sont loin d'être insatisfaisants. Tout en admettant qu'aucun système n'est totalement sûr, M. Éric Trappier a estimé que l'épée et le bouclier « *évoluent en parallèle* » et indiqué que les avions militaires étant d'ores et déjà conçus pour ne pas « tomber » en cas de piratage informatique. M. Stéphane Mayer a lui aussi assuré que tout équipement intègre des capacités de fonctionnement en mode dégradé. M. Patrick Hebrard a précisé que la marine nationale ayant pour objectif que les équipages soient le plus autonomes possibles, il est prévu, en cas de défaillance d'un système numérique, des **mécanismes manuels de sortie de situations délicates**. M. Paul Théron a cependant estimé que de telles possibilités de fonctionnement « en mode dégradé » n'existent pas pour toutes les plateformes de façon aussi systématique ; par exemple, la propulsion des FREMM dépendrait du bon fonctionnement d'un système simple qui ne serait pas invulnérable.

b. Une préparation opérationnelle aux opérations en « mode dégradé »

M. Gérard de Boisboissel a fait valoir l'importance du défi que l'exigence de résilience fait peser sur les responsables de la formation des militaires. En effet, les personnels doivent être formés et entraînés à la fois au maniement des équipements modernes et aux mêmes usages « en mode dégradé ».

En cela, la numérisation a schématiquement pour conséquence un **doublement des temps et des coûts de formation et de préparation opérationnelle**, auquel il n'est pas certain que le dispositif actuel de formation des militaires soit adapté.

2. Opérer « en mode dégradé » pour gagner la guerre, contre l'*hybris* de l'hyper-technologie

Si les progrès de la révolution numérique sont indéniablement prometteurs pour les armées, les rapporteurs n'en tiennent pas moins à en replacer l'étude dans une analyse plus globale des opérations militaires. Il y aurait en effet une forme de « myopie stratégique » à borner une analyse des enjeux de la numérisation des armées à une prospective technologique, mesurant autant que faire se peut les capacités nouvelles ou accrues de tel ou tel équipement sur le plan tactique, sans se demander si, *in fine*, la technologie concourt effectivement à la victoire stratégique. Toute réponse manichéenne à cette question serait naturellement excessive, donc trompeuse. Mais il importe de ne pas présenter la numérisation des armées comme promettant davantage que ce qu'elle offre : des moyens technologiques accrus.

Ces capacités technologiques accrues sont-elles toujours indispensables ? Comme l'a dit faut observer M. Joseph Henrotin, **une évolution technologique n'avait réellement de sens, même au plan tactique, que si elle confère un surcroît de liberté de manœuvre** aux forces. Il a pris l'exemple des premiers travaux sur le « soldat du futur », conduits par l'OTAN à la fin des années 1980, qui se sont traduits en France par le programme de fantassin à équipements et liaisons intégrés (FELIN). « ***Félin sert-il vraiment ?*** *La gestion de cette opération d'armement reposait-elle, comme critère déterminant, sur la valeur ajoutée qu'un soldat de l'infanterie y trouve ? Ce n'est pas certain* ».

Ces capacités technologiques accrues sont-elles toujours bénéfiques ? Comme le dit le chercheur précité, **la numérisation peut au contraire engendrer « *des œillères* »** : les cahiers du centre de doctrine et d'enseignement du commandement montrent bien qu'il ressort d'une ou deux décennies de numérisation que « ***ce n'est pas un miracle en soi*** ». La **révolution numérique peut même devenir un piège**, par un phénomène de contrainte, d'« abonnement » des armées à des développements technologiques rapides et coûteux, voire de dépendance à ces équipements parfois vulnérables.

À cet égard, le retour d'expérience des guerres conduites dans les années 2000 par des puissances à très haut potentiel technologique laisse dubitatif – on pense non seulement aux campagnes américaines en Irak et en Afghanistan, mais aussi, par exemple, à l'opération israélienne de 2006 dans le sud du Liban.

Certes, il serait imprudent d'exclure l'hypothèse d'un affrontement entre deux puissances de niveau technologique comparable. Dans un tel scénario de conflit, nos armées auraient évidemment intérêt à ce que le différentiel technologique ne soit pas en leur défaveur. Mais même dans ce type de scénarios de crise, comme l'a fait valoir la commissaire générale Françoise Latour pour le cas – emblématique – de l'aviation de combat, **à budget identique, un arbitrage équilibré doit être trouvé entre** :

– **la sophistication technologique d'un modèle de matériel**, qui va croissant avec ses prix unitaires ;

– la quantité d'équipements qui forment la masse de bataille.

En somme, il ne faut attendre de la numérisation que ce que peut promettre la technologie dans la guerre : un avantage tactique, mais pas toujours, et jamais plus.

IV. LA NUMÉRISATION DES ARMÉES POSE *IN FINE* LE PROBLÈME DE LA « SOUVERAINETÉ NUMÉRIQUE »

Dans l'économie numérique, se détachent nettement trois puissances technologiques majeures : les États-Unis, Israël et la Chine. La France n'en fait objectivement pas partie mais elle possède encore des atouts technologiques :

– en matière d'équipements physiques (*hardware*), par exemple avec STMicroelectronics, dernière fonderie européenne ;

– en matière de compétences, comme en atteste par exemple le fait que les ingénieurs français sont très présents dans les effectifs des grands groupes américains, y compris parmi les concepteurs de logiciels de la société Palantir.

Lorsque des équipements numériques – qui ne sont par nature pas imperméables à toutes sortes de détournements – sont utilisés pour des usages aussi stratégiques que ceux des armées, voire des services de renseignement, la maîtrise des technologies numériques constitue bel et bien une question de souveraineté. La maîtrise du numérique se révèle en effet devenir un enjeu de puissance, dans lequel la France ne saurait assister en spectatrice impuissante à une compétition essentiellement sino-américaine. Il est encore possible de consolider nos atouts pour rester « dans la course », soit par des choix nationaux pertinents, soit – lorsque jouent des effets d'échelle trop importants – par des coopérations européennes pragmatiques.

A. AVEC LE NUMÉRIQUE, LA MAÎTRISE DES TECHNOLOGIES EST PARTICULIÈREMENT CRUCIALE POUR L'AUTONOMIE STRATÉGIQUE

Tant pour des raisons de cybersécurité que de dépendance technologique ou même de normes et de standards, la maîtrise des technologies numériques est devenue un enjeu de puissance. Dans cet espace de compétition, la préservation de notre autonomie stratégique suppose de consolider nos atouts par une politique industrielle résolue.

1. Les technologies numériques deviennent des outils de puissance dans la confrontation de grandes puissances

Comme le dit bien notre collègue Cédric Villani, « *le cœur politique et économique de l'intelligence artificielle bat toujours dans la Silicon Valley, qui fait encore office de modèle pour tout ce que l'Europe compte d'innovateurs* ». Pour lui, « *plus qu'un lieu, davantage qu'un écosystème particulier, elle est, pour beaucoup d'acteurs publics et privés, un état d'esprit qu'il conviendrait de répliquer* » ; ainsi, « *la domination californienne, qui subsiste dans les discours et dans les têtes, nourrit l'idée d'une voie unique, d'un déterminisme technologique* ».

Cette situation peut être vue comme plaçant d'ores et déjà la France en position de « **colonie numérique** » des États-Unis, selon l'expression employée il y a déjà cinq ans par un rapport d'information sur la place de l'Union européenne dans le monde numérique [(1)].

a. Les technologies numériques constituent aujourd'hui des outils de soft power pour les grandes puissances technologiques

Les grandes puissances consentent des investissements massifs, souvent encouragés ou directement dirigés par leurs États, dans les technologies numériques. Ainsi, Mme Frederick Douzet a fait valoir que la Chine, par exemple, a élaboré une stratégie numérique qui comporte notamment une politique d'investissement visant à porter le marché de l'intelligence artificielle à 150 milliards de dollars d'ici 2020, irriguant ainsi la recherche, l'industrie et les administrations dans une constante recherche d'innovation. Ce plan – spectaculaire par les montants financiers avancés – s'inscrit manifestement dans une **stratégie de contestation de la domination américaine** dans le secteur des technologies numériques en général et de l'intelligence artificielle en particulier. C'est de ce même champ technologique que, rapporte notre collègue Cédric Villani, le président Vladimir Poutine a quant à lui affirmé que « *celui qui deviendra le leader dans ce domaine sera le maître du monde* », établissant un parallèle entre l'intelligence artificielle aujourd'hui et le secteur nucléaire il y a quelques décennies. Pour l'heure, l'industrie numérique américaine demeure la plus performante du monde ; les interlocuteurs des rapporteurs à Washington ne lui voient souvent comme concurrent crédible, sur l'ensemble du spectre des technologies numériques, que l'industrie chinoise.

Les rapporteurs se sont en effet attachés à étudier en détail les rapports du gouvernement américain – particulièrement le *Department of Defense* – avec l'industrie numérique. Comme en conclut l'étude précitée de l'*Eisenhower School* présentée aux rapporteurs, on pourrait résumer la politique numérique des États-Unis de la manière suivante :

– le gouvernement américain s'y assigne trois rôles principaux : **éviter une cyberattaque** majeure ; assurer la **domination américaine dans le cyberespace** ; promouvoir la **digitalisation de l'économie** mondiale comme un élargissement des débouchés commerciaux de ses entreprises ;

– il privilégie les logiques de **partenariat entre l'État et les entreprises privées**, qui gèrent 85 % des infrastructures critiques, et n'a recours à ses pouvoirs de réglementation qu'à défaut de partenariat ;

– il constitue lui-même un **client majeur de l'industrie numérique américaine**, comme le présente l'encadré ci-après ;

---

(1) Rapport d'information n° 443 de Mme Catherine Morin-Desailly, fait au nom de la commission des Affaires européennes du Sénat, mars 2013.

– il tend à **se servir du numérique comme d'un outil de puissance** parmi d'autres, d'une part en tenant un rôle déterminant dans la définition des standards et des normes et, d'autre part, en consentant des efforts substantiels d'éducation de la population à l'« hygiène cybernétique » pour limiter les vulnérabilités numériques de la société américaine.

Le *Department of Defense*, client majeur de l'industrie numérique américaine

1. Une industrie de grande taille et un client disposant de budgets d'investissement massifs

Du côté de la demande, les États-Unis dépensent, en moyenne, 600 milliards de dollars pour la défense – soit 3,4 % de leur PIB –, dont 120 milliards de dollars pour les acquisitions d'armements et **70 milliards de dollars en R&D**. Ce budget tend d'ailleurs à croître depuis 2016.

Du côté de l'offre, selon l'étude précitée de l'*Eisenhower School*, l'industrie américaine des technologies d'information et de communication (TIC) se compose, pour 19 % du chiffre d'affaires, de sociétés de services informatiques, pour 27 % de fournisseurs d'équipements physiques d'information et de communication (*hardware*), pour 13 % de producteurs de logiciels (*software*) et pour 41 % de fournisseurs d'accès aux services de télécommunication. L'ensemble produit un **chiffre d'affaires cumulé mondial de 3 400 milliards de dollars** en moyenne, dont le taux de croissance annuelle s'établit généralement entre 3 % et 4 %. 99,7 % des sociétés du secteur comptent moins de 500 employés. Ces sociétés se répartissent en **trois secteurs d'activité principaux : la cybersécurité, le *cloud*, et les services de télécommunication**.

2. D'importants achats de matériels et de services informatiques

D'après les indications de M. Carl Schonander, directeur des affaires internationales de la *Software & Information Industry Association* (SIIA) – syndicat des industries des technologies de logiciels et de l'information –, **toutes les grandes entreprises du secteur du logiciel travaillent avec le *Department of Defense*** ; si l'existence de ces liens n'est pas un secret, leur teneur et la nature des données partagées sont par nature moins publiques.

À titre d'exemple, les représentants du *Center for Cognitive Government* d'IBM rencontrés à Washington ont ainsi indiqué que le *Department of Defense* est un des clients majeurs d'IBM. Cette société vend à la fois des produits et des services, notamment de mise à jour, mais ce ne sont pas ses personnels qui opèrent ses applications pour le compte du département – dans d'autres pays, toutefois, IBM fournit des services plus « *opérationnels* ». En outre, comme tel est souvent le cas dans l'industrie américaine, l'un de ces **cadres dirigeants** d'IBM rencontrés par les rapporteurs a été officier de marine, affecté à des fonctions de renseignement, et reste réserviste.

Le Pentagone se fournit **quasi-exclusivement auprès d'industriels américains** pour ses programmes numériques. On notera d'ailleurs qu'avec des groupes comme Google, IBM, Microsoft ou *Amazon Web Services*, il n'est pas captif d'un fournisseur unique.

Certes, en apparence, les crédits publics de soutien à la recherche sont concentrés sur la recherche fondamentale. Comme l'a dit le colonel Paul Gillespie, professeur à la *Dwight D. Eisenhower School for National Security and Resource Strategy*, « ***l'idée générale des autorités américaines est de concentrer le financement public sur la recherche fondamentale**, laissant au secteur privé l'essentiel du financement de la recherche appliquée* ». Telle est la logique de

fonctionnement de la DARPA, mais aussi des différents « labs » du *Department of Defense*. Parmi les instruments utilisés par le gouvernement pour soutenir la recherche fondamentale, il a cité : les travaux de la DARPA ; des bourses allouées aux chercheurs dans les universités américaines ; des aides à la publication ; le financement sur fonds publics de laboratoires de recherche ; et le dispositif de *Private Capital Funds*, mécanisme par lequel le *Department of Defense* finance des travaux de recherche et technologie classés en six catégories de niveau de maturité scientifique ou technologique de leur objet, entre lesquelles le ministère vise à établir un équilibre qui ne soit pas défavorable à la recherche très « amont ».

Néanmoins, les rapporteurs ont pu mesurer l'importance de **transferts mutuellement bénéfiques entre l'administration américaine et les industriels du numérique**, que présente l'encadré ci-après. Ils relèvent notamment l'intérêt :

– de dispositifs **permettant à des entreprises privées d'accéder à des jeux de données des armées**, qui constituent la « matière première » de nombre de développements technologiques, conférant ainsi à l'industrie numérique américaine un sérieux avantage compétitif ;

– le ***Defense Innovation Unit experimental***, service du *Department of Defense* constitué d'antennes placées au cœur des grands écosystèmes de R&D numérique, notamment dans la *Silicon Valley*, avec pour mission de repérer et de soutenir des *start-up* intéressant le Pentagone.

Des transferts mutuellement bénéfiques entre l'administration américaine et les industriels du numérique

1./ Le *Department of Defense* contribue à alimenter la R&D privée

a) La fourniture de données

Interrogés par les rapporteurs sur le point de savoir comment les industriels américains du numérique se procurent les considérables masses de données nécessaires pour rôder leurs produits de gestion du *big data*, d'intelligence artificielle ou de *machine learning*, les représentants d'IBM ont expliqué que **le *Department of Defense* peut fournir « *sans grande difficulté* » et à titre gratuit des bases de données** qui présentent le double avantage d'être constituées de données **non seulement réelles, mais aussi actuelles**. L'industriel dispose ainsi des données lui permettant d'affiner ses technologies et de donner à ses produits une certaine crédibilité ; le Pentagone bénéficie quant à lui de l'exploitation gratuite de ses données.

La procédure employée, appelée *Cooperative Agreement*, repose sur une logique de partenariat public-privé ; elle permet au ministère d'encadrer l'usage fait de ces données par son cocontractant. Ces contrats peuvent prévoir que les algorithmes et autres produits ainsi développés font l'objet de droits exclusifs d'utilisation au profit du *Department of Defense*, le plus souvent pour une période limitée à l'issue de laquelle ils peuvent être commercialisés.

b) Les transferts de « briques » technologiques

Le *Department of Defense* cherche à se rapprocher des *start-up* avec l'organisation de défis et de « labs », comme avec l'ouverture de bureaux spécialisés, à l'image du DIUx implanté dans la Silicon Valley, à Austin (Texas) et à Boston (Massachussets). Le DIUx a pour mission de repérer des *start-up* susceptibles de fournir au Pentagone des technologies

numériques dans de meilleurs délais que les grands groupes. Il est investi à cette fin du pouvoir de mettre en œuvre des dispositifs de contractualisation variés – y compris des prises de participation.

Selon les explications fournies aux rapporteurs à l'*Eisenhower School*, ce type d'interfaces procède d'« *une sorte de mélange de cultures, entre celle du Gouvernement et celle du capital-risque* », et tant le ministère que les *start-up* y trouvent intérêt. En effet, le *Department of Defense* possède des compétences technologiques exploitables par le secteur privé, mais ne possède pas souvent les compétences pour les valoriser. Ainsi, certains freins réglementaires ont été progressivement levés en vue de **favoriser le transfert de technologie du secteur public à l'industrie privée**. Les *start-up* concernées peuvent ainsi exploiter une part du capital technologique du Pentagone, moyennant des *royalties* en faveur de celui-ci.

2./ L'innovation numérique revêt un caractère « itératif » assumé

Les industriels du numérique soulignent le caractère « itératif » des développements numériques opérés par le secteur privé pour le *Department of Defense*.

IBM observe ainsi que l'intelligence artificielle et la doctrine (au sens large) du ministère évoluent de façon itérative. En effet, les développements civils de **l'intelligence artificielle créent des usages nouveaux pour le *Department of Defense*, qui permettent à leur tour de perfectionner cette technologie**.

Par exemple, IBM développe des systèmes d'intelligence artificielle, sous le nom commercial de Watson, pour tous types de clients. Certains industriels du secteur des hydrocarbures, par exemple, ont voulu utiliser Watson pour l'évaluation et la gestion des risques afférents à certains de leurs investissements. Pour ce faire, IBM a visé à recueillir l'ensemble des données disponibles dans le pays où un tel investissement était envisagé – actualités, médias sociaux, etc. – et leur a appliqué ses technologies d'intelligence artificielle pour analyser la situation et proposer des scénarios de décision ; « *dans le fond, cela s'apparente à un système de* Command and Control *(C2)* ». Le *Department of Defense* a souhaité tester cette technologie pour certaines de ses études et a passé à cette fin un contrat d'expérimentation avec IBM, pour 200 000 dollars. IBM a alors collecté de considérables masses de données sur les Philippines et employé ses outils d'intelligence artificielle pour analyser l'évolution de l'influence relative de la Chine et des États-Unis dans ce pays – il en ressortait que l'influence chinoise était grandissante. Dans ce cas, le Gouvernement a trouvé intérêt à l'analyse de l'information, et IBM au perfectionnement de ses technologies.

Amazon Web Services fait valoir que l'un des enjeux des contrats de fourniture du *Department of Defense* auprès de l'industrie privée consiste à « ***nourrir l'innovation de façon participative*** », car les externalisations donnent aux personnels du ministère et de l'industriel l'occasion de discuter et, ainsi, de découvrir de nouveaux usages des technologies. De même, la coopération avec les agences de renseignement a « ***un côté itératif*** *: la solution informatique évolue de façon incrémentale* ».

3./ L'impact de la réglementation

a) L'impact direct d'une normalisation « souple » sur les conditions de la R&D

De façon générale, les cadres d'*Amazon Web Services* ont souligné que l'innovation suppose parfois une certaine souplesse dans la réglementation ou l'application de celle-ci.

Les rapporteurs ont étudié à l'*Eisenhower School* les équilibres qui se dessinent ainsi dans l'élaboration des normes de la « 5G »), qui doivent concilier :

– l'impératif de résilience des réseaux, qui conduit les administrations à privilégier des standards robustes et assez détaillés ;

– le souci d'exploiter au mieux les possibilités technologiques de ce que la SIIA voit comme la plus importe rupture technologique à venir dans les trois à cinq ans du fait des vastes usages nouveaux qu'elle peut permettre, qui plaide en faveur de normes aussi souples que possible.

b) L'impact indirect d'autres pans de la législation

● Le **droit de la protection des données personnelles** a plusieurs fois été évoqué comme un des adjuvants de l'innovation numérique ; c'est d'ailleurs l'un des thèmes d'études de l'*Eisenhower School*. Pour la SIIA, la relative souplesse du droit américain de la protection des données privées « *a pu aider la croissance de certains industriels, comme* Google *ou* Facebook » ; l'actualité récente ne paraît pas lui donner tort sur ce point. En effet, comme l'a expliqué schématiquement M. Carl Schonander, à l'inverse des régimes juridiques européens, le droit américain, schématiquement, applique le secret par exception plutôt que par principe.

Selon l'étude précitée de l'*Eisenhower School*, trois postures-types existent en matière de gestion des données personnelles :

– la maîtrise centralisée des données, dont la Chine est le parangon : l'internet y repose sur neuf routeurs principaux, gérés par l'État, et les réseaux sociaux y font l'objet d'un strict contrôle, passant même par des systèmes de récompense pour les Chinois qui contribuent à la propagande de leur gouvernement dans l'espace numérique ;

– le primat donné à la liberté de collecter les données sauf interdiction expresse, comme c'est schématiquement le cas aux États-Unis ;

– un encadrement strict de la collecte de données, voie choisie par l'Europe.

● Ces modèles ont des **implications concernant la localisation des données** : ils sont plus ou moins attractifs pour l'industrie numérique, dans les cas où celle-ci est libre d'implanter ses serveurs où elle le souhaite.

La SIIA plaide pour « *une certaine interopérabilité des systèmes de droit* », à l'image de ce que prévoit l'accord entre les États-Unis et l'Union européenne connu sous le nom de *Privacy Shield*. Elle estime que si la fragmentation du droit n'est pas le système le plus productif, le plus important est que l'industrie numérique puisse continuer à traiter les données là où elle le veut, sur les mêmes serveurs quelle que soit leur provenance – quitte à appliquer des droits différents aux différentes données –, plutôt que d'être obligée de stocker les données dans un serveur miroir local – comme l'exige par exemple le Brésil. Ainsi, **l'industrie américaine a davantage intérêt à des « *systèmes d'interopérabilité juridique* » qu'à des obligations de localisation des données**.

● Le SIIA reconnaît que le ***Foreign Intelligence Surveillance Act*** de 1978 et un ensemble d'autres règles fédérales s'appliquent à tous les acteurs de l'industrie numérique présents aux États-Unis. L'idée générale sous-tendant ce *corpus* de normes est de permettre à la Justice et aux services de renseignement de « *coopérer avec les sociétés informatiques de façon fructueuse* ».

Mais il relève aussi que, si les Européens sont souvent critiques envers les autorités américaines quant à leurs intentions envers les données hébergées aux États-Unis, même par des acteurs privés, ils sont moins critiques envers les autres Européens, alors qu'ils n'auraient peut-être pas toujours moins de raisons de l'être.

Voilà pourquoi notre collègue Cédric Villani conclut à juste titre que « *dans la mesure où les chaînes de valeur, surtout dans le secteur numérique, sont désormais mondiales, les pays qui seront les* leaders *dans le domaine de l'intelligence artificielle seront amenés à capter une grande partie de la valeur des systèmes qu'ils transforment, mais également à* ***contrôler ces mêmes systèmes, mettant en cause l'indépendance des autres pays*** ».

b. Une position dominante sur un marché technologique se traduit par une standardisation qui freine la concurrence

i. Une standardisation *de facto* des outils numériques qui aboutit à généraliser des standards d'entreprises américaines

Dans l'économie numérique, les effets d'échelle à l'œuvre et l'intensité des échanges d'informations conduisent souvent l'ensemble des acteurs à adopter un même standard. Lorsqu'elles ne sont pas à l'origine d'un développement technologique, « *la France et l'Europe n'auraient d'autre choix que de prendre le train en marche* », comme le dit notre collègue Cédric Villani. Les illustrations de ce phénomène sont nombreuses : il suffit pour s'en convaincre de voir le ministère des Armées compter Microsoft parmi ses fournisseurs ou de voir la direction générale de la sécurité intérieure (DGSI) utiliser des logiciels fournis par Palantir – une société américaine financée par un fonds bien connu pour être lié à la CIA.

Notre collègue Cédric Villani met aussi en lumière cette même dynamique dans le secteur de l'intelligence artificielle, avec par exemple, en matière de *deep learning*, des technologies comme *TensorFlow* (développée par *Google*), « *qui ont été adoptées, dès leur ouverture, par l'écrasante majorité du marché, que ce soit les industriels, les* start-up *ou les académiques* ». Certes, la généralisation de ces « briques de base » leur évite « *de réinventer sans cesse les mêmes solutions* », mais « *elles contribuent à* ***imposer un standard de fait*** », ce qui « ***peut s'avérer préjudiciable*** » si leurs inventeurs, « *qui restent les bénéficiaires, décidaient de récupérer l'ensemble des développements* » conduits avec ces « briques ».

Pour notre collègue Cédric Villani, « *on observe la même tentation chez les entreprises européennes qui, persuadées d'avoir déjà perdu la course, cèdent bien souvent aux sirènes des géants de la discipline, parfois au détriment de nos pépites numériques* ». Cet aspect de la standardisation *de facto* est d'autant plus regrettable que **nombre de développements ne seraient pas hors de portée pour la R&D et l'industrie françaises**. Ainsi, pour citer un cas particulièrement épineux, l'ensemble des experts consultés par les rapporteurs s'accorde à estimer que développer un « Palantir français » pour équiper nos services de renseignement n'aurait rien d'insurmontable pourvu, comme l'a souligné le directeur général de l'INRIA, que soient remplies deux conditions :

– que les commanditaires de matériels « souverains » traduisent explicitement, dans leurs spécifications industrielles, les impératifs régaliens en exigences précises de confidentialité et de souveraineté technologique ;

– que ces mêmes commanditaires consentent les investissements cohérents avec ces exigences.

ii. Des efforts de standardisation *de jure* qui se traduisent souvent par l'adoption de standards américains, notamment en matière militaire

M. Brian Teeple, adjoint de la *Chief Information Officer* du Pentagone en charge des fonctions de « C4&IIC » – pour *Command, Control, Communications & Computers* (C4) et *Information Infrastructure Capabilities* (IIC) – a expliqué que les États-Unis promeuvent, au sein de l'OTAN, un effort de standardisation de ces équipements, notamment les communications satellitaires, pour lesquelles l'Alliance a investi un milliard de dollars depuis une quinzaine d'années.

Si l'interopérabilité des équipements entre Alliés possède indéniablement des vertus opérationnelles, ses bénéfices sont moins mutuels lorsqu'elle repose sur l'adoption par tous les Alliés des technologies fournies par un seul et même d'entre eux. Ainsi, **la standardisation peut revêtir un caractère hégémonique**.

D'ailleurs, la commissaire générale Françoise Latour a établi un intéressant parallèle entre les services des GAFA et l'avion de combat furtif F35 Lightning, qui sera aussi adopté par plusieurs autres États membres de l'OTAN. En effet, « *le standard technologique très avancé et fermé du F35 en fait un vecteur commercial hégémonique* », qui risque fort de « *mettre en difficulté les industries aéronautiques européennes* ». Nombre d'éléments de l'appareil sont en effet placés sous le contrôle des seuls Américains ; les standards de l'aviation de combat de cinquième génération s'en trouvent donc largement fixés par eux. De plus, le choix du F35 a pour effet de structurer l'écosystème de R&D de ses acheteurs, à tel point qu'il fait peser une hypothèque sérieuse sur leur capacité à développer des programmes de remplacement de leurs autres flottes. En outre, pour les pays acquéreurs, il sera très difficile d'engager leurs avions sans l'aval américain. Ainsi, effet d'« assèchement » de la R&D européenne et « effet de standard » jouent aujourd'hui de façon inquiétante.

C'est pourquoi, dans le secteur du numérique et plus particulièrement pour l'intelligence artificielle, notre collègue Cédric Villani plaide en faveur d'une **réduction des phénomènes de monopole et des logiques d'enfermement dans certains standards**. « *Il s'agira en particulier, dans une démarche proactive et coordonnée, d'établir et d'imposer des normes d'interopérabilité non-propriétaires, ainsi que des sorties locales pour les dispositifs producteurs de données personnelles et non personnelles* ».

c. L'acquisition de technologies étrangères fait peser un risque de dépendance, pour leur réexportation voire pour leur emploi

L'état-major de l'armée de l'air a fait valoir qu'une acquisition étrangère peut conduire à :

– un certain degré de contrôle des autorités du pays vendeur concernant l'emploi de la machine, par exemple pour l'accès aux pièces de rechange ou aux mises à jour ;

– à l'existence de « **barrières propriétaire** », par exemple des zones de *black-out*, la commissaire générale Françoise Latour citant l'exemple (purement théorique) d'un avion qui éteindrait automatiquement ses capteurs lorsqu'il survole le territoire d'un allié précieux des Américains. Rien de tel cependant avec l'AWACS : l'armée de l'air n'a jamais décelé de telles barrières, peut-être parce que l'AWACS est « interfacé » avec de nombreuses plateformes européennes.

M. Éric Trappier a d'ailleurs souligné « ***la volonté des Américains de contrôler le traitement de l'information*** » dans l'emploi que font leurs alliés des matériels de fabrication américaine. Schématiquement, comme il l'a expliqué, les États-Unis sont tout disposés à donner à leurs alliés un accès à leurs capacités de traitement des données, mais ne les laissent pas « entrer » dans ces capacités : « *ils fournissent la connexion, pas le cerveau* ». Par exemple, avec le drone *Reaper*, non seulement le modèle de l'appareil est américain, mais surtout, toutes les données captées par le drone sont traitées aux États-Unis ; en outre, l'entretien des machines fait intervenir des personnels accrédités par les États-Unis.

Une telle dépendance peut cependant être délibérément acceptée, ou ne pas brider l'usage que l'on fait du matériel acquis à l'étranger. Mais intégrer des puces américaines, même dans un missile, expose au risque d'interdictions strictes d'exportation au titre de l'***International Traffic in Arms Regulations*** (ITAR). Cette législation commerciale américaine, qui a trait au contrôle des importations et exportations intéressant la défense, est en effet d'application extraterritoriale. Aussi l'exportation de produits français comportant des « briques » numériques américaines pourrait être interdite par l'administration américaine.

S'agissant plus particulièrement des logiciels, un risque supplémentaire existe. En effet, comme l'a expliqué le directeur général de l'INRIA, tout logiciel peut collecter « *des masses très surprenantes de données* », ce qui en fait un vecteur efficace de renseignement. C'est pourquoi « ***dans le monde numérique, on peut moins encore que dans d'autres industries se fier à un produit étranger*** ». Un matériel dépourvu de systèmes d'information – comme, par exemple, le successeur du FAMAS – ne sera assurément pas vicié, mais un logiciel peut toujours l'être. On notera d'ailleurs que cette difficulté se pose même aux États-Unis. Ainsi, en mai 2018, le *Department of Defense* a pris la décision d'interdire à la vente dans les magasins des bases militaires américaines les *smartphones* des marques chinoises Huawei et ZTE en raison « *des risques de sécurité inacceptables présentés par ces appareils* ».

d. La maîtrise des technologies acquises à l'étranger constitue la dernière garantie d'autonomie nationale

Le directeur du renseignement militaire a indiqué que son service a étudié le logiciel de la société américaine Palantir, mais qu'il ne l'a pas retenu pour des questions de maîtrise du logiciel. La maîtrise des expertises et des compétences est en effet indispensable ; elle justifie d'ailleurs que chaque service teste tous types de produits.

En effet, lorsque les armées ou les services de renseignement n'ont d'autre choix que d'acquérir des équipements numériques « sur étagère », elles doivent s'attacher à maîtriser l'ensemble de ces équipements. Comme l'a souligné un haut responsable d'un service de renseignement, la préservation de notre souveraineté ne passe pas nécessairement par la fabrication sur le territoire national de l'ensemble de nos équipements, mais elle **exige de leurs utilisateurs soit une compréhension absolue de leur fonctionnement soit, à défaut, un usage de ces équipements sans aucune connexion** avec le reste du « monde numérique ». La préservation de la souveraineté consiste donc à disposer *a minima* d'ingénieurs qui assurent la maîtrise des systèmes.

L'essor du logiciel libre est à cet égard favorable, car comme l'a expliqué Mme Isabelle Ryl, un logiciel libre est souvent plus sûr qu'un logiciel privé dans la mesure où, dès lors que son code est public, il est scruté par un grand nombre d'experts, ce qui facilite la découverte d'éventuels « chevaux de Troie ».

2. La souveraineté numérique suppose de conserver ou de (re)conquérir des atouts technologiques

Compte tenu des risques de dépendance technologique et des dangers qui s'y attachent, il est légitime, comme le dit bien notre collègue Cédric Villani, « *de ne céder à aucune forme de déterminisme* ». Or, en matière numérique, « *le jeu du marché seul montre ses limites pour assurer une véritable politique d'indépendance* » et, d'ailleurs, l'ouverture des marchés intérieurs ne sert pas toujours les intérêts économiques des États européens, « *qui l'appliquent trop souvent à sens unique* ».

Pour les rapporteurs, c'est sans complexe que l'État peut – et doit – s'engager dans une politique volontaire de protection et de développement de nos atouts technologiques. Cette politique, qui commence par un soutien résolu au développement de solutions françaises dans les secteurs les plus risqués du point de vue de la souveraineté technologique – comme les logiciels opérationnels des armées, directions et services –, doit exploiter tous les moyens envisageables pour soutenir notre BITD dans le secteur du numérique.

a. Soutenir la constitution d'une offre souveraine pour répondre à des besoins d'équipements numériques sensibles

Les procédures actuelles d'acquisition d'équipements pour nos armées, si elles sont utilisées avec toute la souplesse que leurs textes permettent, autorisent d'ores et déjà à soutenir la constitution d'une offre française pour répondre aux besoins des armées les plus sensibles dans le domaine numérique. Par ailleurs, pour des applications plus simples, logiciels libres et développements internes peuvent offrir d'intéressantes possibilités. En tout état de cause, il appartient à l'État en général et aux armées en particulier de « donner l'exemple », en évitant autant que possible de se fournir auprès de prestataires étrangers pour des équipements, des logiciels ou des services que notre industrie numérique pourrait développer elle-même.

i. Réserver les usages sensibles à des logiciels « souverains »

Interrogé sur la doctrine de la DGSIC en matière de recours à des logiciels « non souverains », l'amiral Arnaud Coustillière a expliqué que « ***ce qui est souverain, dans l'espace numérique, ce sont les données et, de plus en plus, l'algorithme qui sert à les traiter*** ».

Selon les explications de l'amiral, les codes de certains logiciels sont mis à disposition du public – ces logiciels dits « libres » ayant indéniablement leurs avantages –, tandis que, pour d'autres, les codes sont conservés par leurs propriétaires. Depuis 2016, le ministère des Armées articule les deux types de logiciels. D'où le choix de Microsoft par trois ministres successifs pour la gestion des réseaux, « *afin d'industrialiser les processus des opérateurs et en particulier les processus de mise à jour ainsi que de déploiement et de reconfiguration* ». D'où, également, le choix d'autres logiciels, en codes libres, très utilisés par exemple par le SGA pour sa transformation numérique, ou dans des champs d'activité où le besoin d'industrialisation des développements logiciels est moindre. L'amiral a souligné que les deux offres sont complémentaires et pas toujours substituables l'une à l'autre : « *on aurait jamais pu organiser le déménagement SIC des 9 500 personnes à Balard sans les outils de Microsoft* ».

Bien entendu, il n'appartient pas aux rapporteurs de dresser une liste exhaustive des logiciels et autres équipements numériques qui ne sauraient être acquis « sur étagère » à l'étranger. Un cas néanmoins leur paraît objectivement problématique : l'utilisation par la DGSI d'un logiciel de gestion d'informations fourni par la société Palantir, détenue par un fonds d'investissement connu pour sa proximité avec la CIA. Pour l'amiral Arnaud Coustillière lui-même, « ***Palantir, c'est hors de question !*** » car ce logiciel est utilisé au niveau de la collecte et du traitement de données relatives au renseignement, donc particulièrement sensibles. L'amiral a d'ailleurs fait valoir que le succès de Palantir a tenu à l'audace d'investisseurs et d'un industriel américain qui ont su prendre quelques risques, alors que certains observateurs regrettent souvent que certains industriels et financiers français ont pour premier réflexe de se tourner vers l'État, pourrait-on

dire en tendant la sébile. Si ce constat n'est pas nécessairement infondé, il convient tout de même de rappeler, pour le cas de Palantir, le soutien du gouvernement fédéral américain, *via* la CIA.

Pour les rapporteurs, il serait légitime **que l'État investisse dans le développement de logiciels français pour ses applications les plus sensibles** – dont la gestion des informations par un service de renseignement constitue l'exemple le plus abouti. Un programme d'armement pourrait contribuer à soutenir le développement des compétences d'un industriel national. Un institut public comme l'INRIA peut d'ailleurs pertinemment être sollicité à cette fin.

ii. Favoriser le recours au logiciel libre et aux développements internes

Pour le même ordre de motifs, **le recours aux logiciels libres et au développement de logiciels en interne mérite d'être favorisé**.

D'ailleurs, comme l'a constaté l'amiral Arnaud Coustillière, l'une des tendances à l'œuvre en matière de « *DevOps* » [(1)] – c'est-à-dire de conduite des projets informatiques – consiste à voir dans le logiciel « *un objet de rapidité, d'agilité* ». À cet égard, le ministère des Armées trouverait intérêt à favoriser les développements d'applications en interne.

Cela supposerait de consolider ses effectifs de développeurs, voire d'en assurer le renfort ponctuel soit par des réservistes, soit par certains de ses personnels qui auraient acquis de telles compétences à titre personnel. Or il semble qu'une certaine tension existe sur la disponibilité de ces compétences. En effet, comme l'a fait valoir le général Bernard Barrera, les armées ont longtemps supprimé ces postes en pensant pouvoir externaliser ces fonctions, mais l'externalisation s'avère ne pas toujours correspondre parfaitement aux besoins de l'armée de terre, être plus coûteuse, et ne pas permettre d'entretenir des compétences en interne. En outre, les développements internes facilitent la prise en compte de l'évolution des systèmes – tel est le cas, de façon manifeste, pour la simulation. Accessoirement, structurer une sorte de « **communauté des développeurs** » du ministère des Armées pourrait permettre de donner une certaine visibilité à ces efforts.

b. Mettre en œuvre tous les leviers dont dispose l'État pour stimuler notre base industrielle et technologique de défense dans le numérique

Sans déroger aux principes fondamentaux du droit de la concurrence, l'État doit pouvoir s'appuyer sur divers outils de politique industrielle pour mettre en œuvre une stratégie résolue de consolidation de nos atouts dans les technologies numériques intéressant les armées. Comme préconisé précédemment, les grands programmes d'armement de nouvelle génération, les moyens propres à

---

(1) Concaténation de l'abréviation « dev » pour l'anglais development *signifiant « développement » et de l'abréviation usuelle « ops » de l'anglais* operations *signifiant « exploitation ». Les deux termes désignent deux fonctions habituellement bien distinctes de la gestion des systèmes d'information, qu'il s'agit, dans l'optique du « DevOps », de réunir autour d'un objectif commun.*

stimuler l'écosystème français de recherche et d'innovation ainsi qu'une refonte des procédures d'acquisition y contribueraient. En plus de ces dispositions, deux mesures transversales permettraient à l'État de soutenir le développement de l'industrie numérique française dans le secteur de la défense : orienter sans complexe la commande publique vers nos entreprises innovantes du numérique et leur fournir des moyens publics de calcul intensif.

i. Mettre en œuvre une stratégie industrielle de soutien au numérique spécifique au secteur de la défense

Les rapporteurs relèvent que la défense et la sécurité constituent l'un des quatre secteurs économiques dans lesquels le rapport précité de notre collègue Cédric Villani recommande de concentrer le soutien de l'État à l'innovation en matière d'intelligence artificielle.

Aux yeux des rapporteurs, c'est à juste titre qu'il plaide contre un saupoudrage des moyens de l'État, estimant préférable de « *tirer parti des avantages comparatifs et des niches d'excellence de notre économie* ». Ce sont là en effet les secteurs dans lesquels notre industrie « *peut sérieusement envisager jouer un rôle de premier plan au niveau mondial* », même face à la concurrence extra-européenne. La défense et la sécurité apparaissent ainsi comme l'un des quatre secteurs prioritaires pour l'investissement public, car il a « *acquis une maturité suffisante pour lancer des opérations de transformation majeures qui nécessitent des investissements importants* ». Ce qui vaut pour l'intelligence artificielle vaut aussi pour le reste des technologies numériques de pointe susceptibles de connaître de véritables ruptures dans les années à venir.

ii. Orienter sans complexe la commande publique de façon à consolider notre base industrielle et technologique de défense dans le numérique

Comme le reconnaît notre collègue Cédric Villani, « *il ne peut y avoir de saine concurrence entre les acteurs européens et les acteurs extra-européens si les premiers ne sont pas en mesure de tenir la course et s'il n'existe pas de réciprocité dans l'accès à la commande publique* ». Or il apparaît clairement que les grandes puissances numériques – les États-Unis et la Chine – ont des marchés publics peu poreux aux offres françaises ou européennes, notamment lorsqu'il s'agit d'achats au profit de la défense. De surcroît, en large partie du fait du soutien apporté par ces puissances à leurs entreprises, l'asymétrie dans l'industrie mondiale du numérique est aujourd'hui trop marquée pour ne pas biaiser le libre jeu de la concurrence.

C'est pourquoi notre collègue Cédric Villani recommande une initiative française afin que le droit européen reconnaisse le droit pour l'autorité adjudicatrice d'un marché public « *de tenir compte de l'état de la base industrielle et technologique européenne pour, par exemple,* ***privilégier un acteur européen lorsque le déséquilibre de la concurrence est manifeste*** ».

Des exceptions de portée comparable sont d'ores et déjà reconnues pour les marchés de défense et de sécurité. Leur mise en œuvre est souhaitable, comme il a été dit, mais son effet économique d'ensemble sur la stimulation de l'offre française ou européenne serait grandement accru si l'ensemble des marchés publics pouvaient être conduits selon des règles telles que le propose notre collègue Cédric Villani.

iii. Développer l'offre publique de moyens de calcul

On l'a dit, la mise à disposition d'un supercalculateur pour le développement des technologies d'intelligence artificielle et l'offre de services de *cloud computing* au sein d'un écosystème de recherche et d'innovation structuré autour du numérique dans le secteur de la défense constituerait à la fois un **catalyseur de l'innovation** et un **facteur de compétitivité**, par les économies qu'il permet dans le développement des produits par simulation numérique – jusqu'à des systèmes de jumeaux numériques qui servent à la fois au développement d'un produit et à la prise de décision en phase de production, voire au stade du MCO d'un équipement.

Les avantages procurés par les moyens de calcul intensif sont bien compris de nombre d'industriels français ; d'ailleurs, selon les dirigeants du GENCI, certains « grands » industriels français sont déjà « *très en pointe* ». Ainsi, Total utilise le calcul intensif et la simulation numérique pour l'exploration des sous-sols – sur le mode de l'échographie –, tant pour l'exploration de gisements que pour l'optimisation de la production. « *Certes, un outil de calcul intensif coûte 50 millions d'euros, mais un forage raté peut coûter jusqu'à 200 millions d'euros* ». De même, Renault aurait gagné cinq ans sur le développement d'un modèle nouveau en simulant ses *crash tests*. EDF utiliserait aussi le calcul intensif pour simuler le comportement des réacteurs nucléaires – y compris en intégrant les réactions potentielles des personnels en cas d'accident.

Pour faciliter l'accès des industriels – « petits » comme « grands » – à des capacités de calcul intensif, **l'utilisation des moyens du GENCI pourrait être rendue possible pour des applications, militaires ou non, ne conduisant pas à des publications mais pour lesquelles la France trouve intérêt à conserver des compétences et un avantage concurrentiel industriels**.

D'ailleurs, si le GENCI devait entrer sur le marché de la location de capacités de calcul, il pourrait être compétitif :

– *Amazon* et *Google* offrent certes aux industriels des capacités de calcul à des tarifs très compétitifs, mais seulement *via* des **formules dites** « **élastiques** », c'est-à-dire que les clients doivent payer bien davantage pour réserver des heures de calcul au moment qui leur convient ; le reste des clients n'est pas prioritaire. De plus, le coût du stockage des données est souvent sous-estimé. Enfin, ces services ne proposent aucun accompagnement technique pour aider les utilisateurs à l'usage des machines ;

– avec le GENCI, l'expérimentateur bénéficie au contraire d'un **accompagnement complet** : les personnels du grand équipement assurent les premiers paramétrages, puis développent une « couche logicielle » supplémentaire avec des logiciels de traitement de données qui permettent d'éviter de nombreuses erreurs et, enfin, partagent leur expérience avec les chercheurs dans l'exploitation des résultats des calculs effectués. Chaque centre de calcul du GENCI compte en effet une quarantaine de spécialistes, capables de discuter avec des scientifiques de haut niveau ; les dirigeants du grand équipement ont estimé que 50 % de la valeur ajoutée de cette infrastructure tient aux personnels qui exploitent les calculateurs. À l'inverse, *Google* ne fournit que l'infrastructure de calcul « nue » ;

– enfin, la **sécurisation des données** constitue « *un vrai problème, pour lequel* Amazon *et* Google *déclinent toute responsabilité* ».

Un système d'accès payant aux moyens du GENCI pour la recherche privée permettrait par ailleurs de mieux financer la nécessaire modernisation des capacités de calcul du Grand équipement. Une machine exaflopique coûterait en effet 200 millions d'euros. Aussi des crédits du troisième plan d'investissements d'avenir, éventuellement abondés par ceux de l'Union européenne, pourraient-ils judicieusement financer l'acquisition d'un calculateur exaflopique, la location d'une part de ces moyens de calcul permettant d'amortir l'équipement et de contribuer à sa maintenance.

Dans le même ordre d'idées, le GENCI pourrait proposer à Atos d'installer sur ses futures machines exaflopiques son simulateur quantique pour permettre aux équipes coordonnées par la cellule de veille technologique du GENCI et aux chercheurs de travailler en amont sur les possibilités offertes par ce type de technologies, par exemple pour évaluer l'adéquation des algorithmes actuels aux futures architectures quantiques.

B. L'ÉCHELLE EUROPÉENNE CONSTITUE PARFOIS LA DIMENSION LA PLUS PERTINENTE POUR LA DÉFENSE DE NOTRE SOUVERAINETÉ

1. L'Europe peut constituer le nouvel horizon de notre autonomie stratégique dans certains domaines technologiques

Pour certaines recherches et certains développements technologiques nécessitant une « taille critique » importante, il peut arriver que des programmes strictement français ne pourraient être financés qu'au prix de renoncements dans d'autres champs de recherches de même importance. Or c'est justement l'un des enseignements de l'expérience de la DARPA que la maîtrise des ruptures technologiques suppose d'investir très en amont dans des champs très variés de recherches sans applications évidentes.

À défaut de solution nationale, la coopération européenne s'impose comme la seule alternative à la dépendance vis-à-vis de puissances extra-européennes. C'est en ce sens que le rapport annexé au projet de loi de

programmation militaire pour les années 2019 à 2025 déclare que « *l'autonomie stratégique qui est au cœur de l'Ambition 2030 est indissociable de la construction d'une autonomie stratégique européenne* ».

a. L'Europe a un poids très significatif dans l'économie mondiale des données, mais pas dans l'industrie numérique

C'est un paradoxe : l'Europe possède un poids majeur dans l'économie mondiale de la production de données et dans la consommation de produits et de services numériques, mais son industrie numérique n'a pas fait émerger de champions mondiaux dans les mêmes proportions.

Ainsi, à titre d'exemple, les représentants de *Facebook* ont indiqué que leur plateforme compte aujourd'hui deux milliards d'utilisateurs, c'est-à-dire de gens se connectant à son service au moins une fois par mois, dont 34 millions en France. Les utilisateurs quotidiens sont plus d'un milliard dans le monde, dont 23 millions en France, sans même tenir compte des autres services de la « famille d'applications » de *Facebook* : *Instagram*, *Oculus*, *WhatsApp* et *Messenger*.

Ainsi, dans l'économie numérique, l'Europe possède une masse critique suffisante, comparable à celle des grandes puissances mondiales. À ce titre, le niveau européen constitue l'échelon le plus pertinent pour conduire certains projets de recherche scientifique et de recherche et développement.

b. La période actuelle offre une occasion historique d'approfondir la coopération européenne

La période actuelle paraît particulièrement propice à ce que les Européens mobilisent collectivement leurs énergies au service de projets nouveaux de coopération dans le champ de la défense et de la sécurité.

En effet, avec la création d'un fonds européen de défense et la constitution quasi-concomitante de la coopération structurée permanente – qui comporte un volet de coopération capacitaire –, l'Union s'est dotée d'outils nouveaux dont il s'agit désormais de se saisir. Le « plan d'action européen de la défense » proposé le 30 novembre 2016 par la Commission et avalisé en décembre par le Conseil européen a en effet ouvert la voie au **financement communautaire des capacités de défense** des États membres.

Le **fonds européen de défense** a pour objet d'aider les États membres de l'Union européenne à « *accroître l'efficacité de leurs dépenses dans les capacités de défense communes, à renforcer la sécurité des citoyens européens et à promouvoir une base industrielle compétitive et innovante* ». Seuls les projets menés par trois États membres au moins seront éligibles à ces financements. Il comporte à ce titre deux volets :

– un **volet de recherche**, au titre duquel l'Union consacrera 90 millions d'euros d'ici 2020 et, par la suite, 500 millions d'euros par an à la recherche dans

les technologies de défense novatrices telles que l'électronique, les matériaux innovants, les logiciels cryptés ou la robotique ;

– un **volet capacitaire** au titre duquel l'Union consacrera, d'une part, deux milliards d'euros d'ici 2020 et, par la suite, quatre milliards d'euros par an au développement de matériels nouveaux ainsi que, d'autre part, 500 millions d'euros d'ici 2020 et, par la suite, un milliard d'euros par an au soutien de l'acquisition en commun des équipements ainsi développés.

Quant à la coopération structurée permanente, elle a été mise en œuvre en décembre 2017, dix ans après que son régime a été institué par le traité de Lisbonne. Le rapport précité du président Jean-Jacques Bridey sur le projet de loi de programmation militaire pour les années 2019 à 2025 présente en détail cette organisation. On soulignera que les programmes conduits dans le cadre de cette coopération bénéficieront d'un taux de cofinancement plus élevé dans le cadre du fonds européen de défense, avec un « bonus » de 10 %. La France participe à dix-sept des vingt premiers projets de coopération décidés par le Conseil le 6 mars 2018. Elle est chef de file de ces coopérations pour deux d'entre eux : le logiciel de sécurisation des radiofréquences (*European Secure Software defined Radio* ou *ESSOR*), qui vise à développer des technologies communes pour les radios militaires européennes, et un projet relatif à la fonction « énergie » en opérations (*Energy Operational Function, EOF*).

Ainsi, la coopération européenne est envisagée comme la meilleure option pour des programmes à forts enjeux technologiques. Encore faut-il, pour que la BITD française bénéficie de retombées des nouveaux instruments européens, que la France sache saisir l'occasion qui s'offre et prendre l'initiative de projets pragmatiques de coopération dans d'autres champs des technologies numériques intéressant la défense.

2. Des coopérations pragmatiques peuvent tirer parti de la « taille critique » de l'Europe pour développer des technologies numériques souveraines

Sans prétendre à l'exhaustivité, les rapporteurs ont recensé plusieurs champs dans lesquels l'échelle européenne paraît pertinente pour développer la base technologique et industrielle d'une véritable autonomie stratégique.

a. La normalisation et la certification des composants informatiques sûrs

M. Paul Théron, titulaire de la chaire Cyb'Air de l'armée de l'air, a évoqué plusieurs chantiers à ses yeux prioritaires « *dans la lignée de la directive NIS* »,[(1)] qui gagneraient à être conduits à l'échelle européenne afin de tirer parti de la « taille critique » de l'Europe :

(1) Directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS » pour Network and Information Security.

– mener des études visant à renforcer la **sécurité informatique** à l'échelle collective, sans s'en remettre trop à l'utilisateur : il y a selon M. Paul Théron un « *biais techniciste, inefficace* » à penser que l'utilisateur « lambda » des technologies numériques adoptera les réflexes adéquats de sécurité informatique, car « *une partie de la population est perdue dans ce monde de complexité abyssale* » ;

– développer des **solutions pour la certification des composants informatiques**. En effet, la Commission européenne promeut la certification de tous les composants, ce qui est « *une excellente idée, car le "ver dans le fruit" n'est jamais à exclure* », mais suppose des moyens importants pour certifier des millions d'objets ;

– M. Paul Théron a rappelé que dans sa communication JOINT (2017) 450 en date du 13 septembre 2017, la Commission Européenne considère que la meilleure façon d'inciter les industriels à assurer la protection cybernétique des objets qu'ils produisent consiste à **établir, en cas de défaillance, des règles de responsabilité** qui les impliquent. La maîtrise de la chaîne de sous-traitants ainsi que la chaîne des responsabilités juridiques constituent également un enjeu très important.

De façon générale, l'Union européenne a toutes compétences pour établir **un cadre réglementaire visant à garantir la sécurité des composants informatiques**, à l'instar des normes qui régissent le marché intérieur.

b. Des investissements capacitaires dans des équipements technologiques de nouvelle génération

Le coût de chaque génération de plateforme ayant tendance à être significativement supérieur à celui de la précédente, les coopérations européennes s'imposent souvent comme la seule alternative crédible et soutenable à l'acquisition sur étagère de matériels américains pour le renouvellement de nos principales plateformes.

Le projet de loi de programmation militaire pour les années 2019 à 2025 énumère déjà plusieurs programmes majeurs que la France a pour ambition de conduire en coopération. Il s'agit notamment de :

– la prochaine génération de char lourd, dit *Main Ground Combat System*, destiné à remplacer les chars Leclerc et Leopard 2 et donc à prendre la place du premier dans la « bulle opérationnelle terrestre » que l'opération SCORPION tend à mettre en réseau ;

– la prochaine génération d'artillerie lourde, avec le projet de *Common Indirect Fire System* ;

– le « système de lutte anti-mines futur », qui est d'ores et déjà conçue comme un « système de systèmes » articulant bâtiments mères de surface, bâtiments base de plongeurs démineurs, drones de surface et drones sous-marins ;

– la prochaine génération de drone de moyenne altitude et de longue endurance (MALE), destinée à remplacer par un système européen les *Reaper* acquis « sur étagère » aux États-Unis faute d'offre française ou européenne structurée en temps utile ;

– le système de combat aérien futur, « système de systèmes » destiné à remplacer le Rafale et présenté *supra*.

Ces projets, ambitieux pour la plupart du point de vue des développements technologiques, concourent à la formation d'une autonomie stratégique européenne et mériteraient à ce titre d'être soutenus par les nouveaux instruments européens de financement.

c. La mutualisation des moyens des Européens pour leur permettre de tenir collectivement leur rang dans la course au calcul intensif

Face aux États-Unis, à la Chine et au Japon, les Européens ont choisi en 2007 de s'unir autour d'une stratégie collective d'investissement dans la mise à disposition de moyens de calcul et le stockage massif de données pour protéger la compétitivité de la recherche scientifique et industrielle européenne. L'encadré ci-après présente l'évolution de cette infrastructure européenne de recherche, appelée PRACE – pour *Partnership for Advanced Computing in Europe*, partenariat pour le calcul intensif en Europe.

Le partenariat pour le calcul intensif en Europe
(ou *Partnership for Advanced Computing in Europe*, PRACE)

Le partenariat pour le calcul intensif en Europe (ou *Partnership for Advanced Computing in Europe*, PRACE) a été créé en 2010 sous la forme d'une association internationale sans but lucratif de droit belge, dont le siège est à Bruxelles. Elle regroupe actuellement vingt-cinq États, et la France y est représentée par le GENCI.

À la création du PRACE, quatre pays dits « membres hébergeurs » (la France, l'Allemagne, l'Espagne et l'Italie) ont accepté d'investir chacun 100 millions d'euros sur cinq ans pour s'équiper, héberger et mettre à disposition de l'ensemble de la communauté scientifique européenne des calculateurs de classe internationale (dits « Tier 0 »). À ce titre, la France a acquis auprès de Bull le supercalculateur Curie, exploité par les équipes de la direction des applications militaires du CEA à Bruyères-le-Châtel et dont 80 % des heures disponibles ont été mises à disposition du PRACE dès 2011.

De 2010 à 2016, ce dispositif a permis à la recherche de disposer de six systèmes de grande taille (dits « Tier 0 ») offrant une puissance cumulée d'environ 20 pétaflops par seconde en 2016.

Une étude d'impact réalisée par le GENCI montre que la France tire pleinement profit de l'infrastructure PRACE :

– **la France est en est le principal utilisateur**, tant au niveau académique qu'industriel, en nombre de projets comme en nombre d'heures ;

– la dimension européenne de PRACE **facilite les collaborations internationales**, qui représentent environ la moitié des projets ;

– quoique difficile à évaluer de façon rigoureuse, le **bénéfice économique** de la coopération pour la France est manifeste ;

– **l'impact industriel est très important**, les industriels français voyant désormais l'utilisation de PRACE, et du calcul intensif en général, comme un argument compétitif majeur.

Un programme **PRACE 2 a été lancé en 2017**, pour une durée de trois ans. Il s'inscrit dans la mise en œuvre progressive d'une stratégie de « marché unique digital » (« *Digital Single Market* »), qui vise à créer un environnement ouvert et sécurisé permettant de générer, traiter, partager et mettre à disposition des données massives pour les communautés scientifiques, les industriels et les collectivités. Cet objectif se décline en deux programmes distincts :

– le programme *European Open Science Cloud* (EOSC), qui vise à mettre en place un ensemble de moyens et de services logiciels en *cloud* permettant l'interopérabilité entre les infrastructures publiques de recherche, en vue de faciliter l'échange et la mise à disposition de données ;

– le programme *European Data Infrastructure* (EDI), qui vise à constituer une infrastructure européenne composée de supercalculateurs interconnectés par des réseaux haut débit, capable de traiter de très gros volumes de données. Ce projet intègre ainsi non seulement des supercalculateurs de PRACE (et donc du GENCI en France), mais aussi les services d'expertise qui y sont associés et les systèmes de transmission réseau spécifiques, l'acteur français de référence en la matière étant Renater.

Ces initiatives visent ainsi à articuler trois composantes de l'écosystème d'exploitation du calcul intensif :

– des **infrastructures fédérées de calcul**, organisées entre les États adhérents à PRACE. C'est dans ce cadre qu'a été élaboré un projet appelé EuroHPC, pour lequel un accord sur un cadre de collaboration a été signé entre treize États le 23 avril 2017 et suivant lequel **l'Union européenne cofinancera en 2020 des machines de niveau « pré-exascale » et, en 2022, deux supercalculateurs exaflopiques**. De ce fait, les États hébergeurs sont aujourd'hui en compétition pour l'accueil de ces infrastructures. La France et l'Allemagne plaident en faveur de l'implantation de l'un en France et de l'autre en Allemagne ; Italiens et Espagnols soutiennent leurs propres candidatures ; même les Luxembourgeois avancent leurs arguments. Considérant **l'enjeu de souveraineté qui s'attache à la localisation de ces équipements**, la France vise à obtenir

l'installation d'un supercalculateur, d'une valeur de 200 millions à 250 millions d'euros, financé à 33 % par l'Union ;

– des **centres d'excellence** développant des applications scientifiques utilisant au mieux ces capacités de calcul, avec par exemple le climat, les matériaux, les nouvelles énergies mais aussi un projet phare de l'Union européenne : la modélisation du cerveau humain dans le cadre du projet « *Human Brain Project* » susmentionné ;

– la **maîtrise de technologies industrielles**, notamment des composants informatiques, dans laquelle la France est le seul pays en Europe à disposer de toute la chaîne industrielle de valeur.

Ainsi, la France a beaucoup à gagner au bon déroulement de l'initiative PRACE 2 et, surtout, à la localisation en France d'au moins un des deux supercalculateurs exaflopiques que l'Union européenne envisage de cofinancer.

d. La reconquête de capacités technologiques et industrielles en matière de processeurs

Les dirigeants du GENCI ont rappelé que pour des composants informatiques aussi cruciaux que les processeurs de pointe, la France reste dépendante de technologies détenues par des pays non européens. Il s'agit notamment des processeurs américains d'Intel ou d'IBM, des accélérateurs de calcul américains de nVIDIA, des équipements de mémoire du coréen Samsung ou de l'américain Micron, ou encore des réseaux de l'israélien Mellanox.

Cette **dépendance technologique** constitue non seulement un manque à gagner industriel, mais surtout une vulnérabilité au regard des enjeux de souveraineté qui s'attachent à ces technologies. L'encadré ci-après en détaille l'étendue. Aujourd'hui, pour la construction de ses supercalculateurs, Atos utilise des composants américains, ce qui permet d'éviter certains composants chinois, mais pas de réduire notre dépendance technologique. D'ailleurs, concernant la provenance des matériels physiques sur lesquels reposent les systèmes d'information – le *hardware* –, les chefs de services de la *Chief Information Officer* du *Department of Defense* ont reconnu qu'il s'agit d'« *un vrai souci en soi* », que le ministère n'a guère d'autre choix que de traiter suivant une logique de gestion du risque.

La dépendance technologique des Européens en matière de composants informatiques

Si les groupes européens parviennent à maintenir une position de force dans certains secteurs tels que les senseurs, en matière de numérique le constat est alarmant : ils ont abandonné le terrain des semi-conducteurs numériques avancés. En conséquence, ils se focalisent sur les objets et les périphériques, délaissant le cœur des systèmes numériques avancés.

De nombreuses initiatives européennes existent pour soutenir l'industrie et sont nécessaires pour le maintien des compétences, mais le constant reste cinglant : **l'Europe n'est aujourd'hui ni souveraine, ni autonome sur l'intégralité de la chaîne de production des composants**. C'est en particulier le cas sur ceux qui apparaissent les plus importants en premier lieu : **les processeurs avancés et la mémoire**. Si on inclut la fabrication comme un élément clé d'indépendance, l'Europe ne dispose ni des technologies ni des moyens de production suffisamment avancés (en termes de finesse de gravure par exemple) pour concurrencer l'Asie. Il en est de même en matière de production de mémoire.

Source : Cédric Villani, mathématicien et député de l'Essonne, « Donner du sens à l'intelligence artificielle – Pour une stratégie nationale et européenne », rapport au Premier ministre, mars 2018.

Le programme *European processor initiative* (EPI) vise à pallier cette dépendance. Projet de collaboration entre dix-neuf partenaires publics et privés, il vise au développement commun de technologies européennes « souveraines » ayant vocation à équiper avec un processeur européen les calculateurs de classe « proto-exascale » et « exascale » qui seront déployés en Europe d'ici 2022. Bull, le CEA, le GENCI et Kalray en sont les membres français. Les dirigeants du grand équipement ont expliqué que la base technologique envisagée pour développer ce processeur européen serait vraisemblablement soit une base appelée ARM, soit une base appelée RISC-V. Ils ont fait valoir qu'il n'était pas anodin que la base ARM, initialement développée au Royaume-Uni, soit désormais la propriété du groupe japonais Softbank qui a récemment acquis *Aldebaran Robotics*, et que si la base RISC-V repose sur des technologies « open source » qui limitent le risque de dépendance, la société qui gère les droits est hébergée dans le Delaware.

Néanmoins, la constitution d'une filière européenne de processeurs, d'abord destinés aux supercalculateurs, est susceptible, par la suite, d'avoir des retombées dans un plus large champ d'application de ces technologies. Parmi les pistes de développement possibles de la technologie des composants, notre collègue Cédric Villani évoque notamment le calcul en mémoire [(1)] et les technologies neuromorphiques [(2)]. Cette initiative mérite donc d'être soutenue et, en cas de succès, développée dans un plus vaste champ de composants.

(1) Technologie en voie de développement consistant à utiliser les propriétés physiques des dispositifs de mémoire à la fois pour stocker et traiter des informations.

(2) Selon le rapport précité de notre collègue Cédric Villani, cette technologie s'inspire de l'organisation interne du cerveau, capable de tâches cognitives impressionnantes avec moins de consommation qu'une ampoule électrique. Ainsi, les systèmes neuromorphiques économisent de l'énergie par rapport aux processeurs et aux cartes graphiques en exploitant deux stratégies :
– ils rapprochent autant que possible calcul et mémoire, limitant les échanges de données ;
– ils effectuent les calculs de manière moins précise que les processeurs, mais plus efficace en énergie.

e. Le soutien européen à la recherche amont

On l'a dit, les méthodes de la DARPA ont fait la preuve de leur efficacité à deux égards au moins :

– l'Agence se concentre sur des projets de recherche à haut risque d'échec, avec des études très en amont de toute application, ce que le lexique en cours dans ce milieu professionnel appelle la ***deep tech*** ;

– ses **méthodes de conduite de projet**, décrites précédemment, lui confèrent une certaine dynamique tout en permettant, de façon quasi incrémentale, d'enchaîner plusieurs projets pour assurer un suivi dans le temps des développements technologiques les plus longs.

On l'a dit également, répliquer la DARPA à l'échelle française serait non seulement hors de portée du point de vue financier, mais également peu efficace dans un pays où l'écosystème de recherche et d'innovation n'est pas comparable à celui des États-Unis.

Faut-il, dès lors, répliquer la DARPA à l'échelle européenne ? Lors de son discours sur l'Europe du 26 septembre 2017, le président de la République a ainsi mis au débat l'idée de créer une **Agence européenne d'innovation de rupture**, chargée de financer des technologies et des sciences émergentes.

C'est en outre sur l'initiative conjointe des rapporteurs que l'Assemblée nationale a adopté, en première lecture du projet de loi de programmation militaire pour les années 2019 à 2025, un amendement au rapport annexé soulignant que, dans le cadre du Fonds européen de défense ou d'autres instruments, un mécanisme européen de financement de projets de recherche et développement à long terme, très en amont de toute application industrielle et dans un vaste champ de technologies de rupture, conférerait aux Européens les moyens de rivaliser avec leurs concurrents.

Indéniablement, le passage à une échelle européenne constitue un enjeu d'autonomie stratégique en matière de recherche et développement. En la matière, l'Europe possède en effet une « masse critique » de technologies et une force de frappe financière qu'aucun État membre, seul, n'a plus. Un soutien accru de l'Union européenne à la *deep tech* est nécessaire.

Pour autant, ce soutien accru doit-il prendre la forme d'une nouvelle agence, centrée sur la défense ? Aux yeux des rapporteurs, la forme que doit prendre cette initiative importe peu ; au contraire, éviter un empilement administratif peut être de nature à ne pas aggraver la charge administrative qui pèse déjà sur les chercheurs. Le débat gagnerait davantage à se porter sur le type d'innovation qu'il convient de soutenir et sur les instruments à mobiliser pour le faire. À cet égard, il convient de distinguer nettement :

– **le soutien apporté aux initiatives proposées spontanément par des chercheurs ou des entrepreneurs**, dans une démarche que l'on pourrait dire « *bottom–up* ». L'Union européenne dispose d'ores et déjà d'une structure dont telle est la mission : le Conseil européen d'innovation, qui a été doté de 2,7 milliards d'euros pour conduire de 2018 à 2020 son premier programme d'intervention pluriannuel ;

– l'orientation de la recherche sur la base de travaux de prospective technico-opérationnelle, dans une démarque que l'on pourrait qualifier à l'inverse de « ***top–down*** », peut-être plus propre à financer des études très en amont d'applications technologiques.

C'est certainement dans ce champ que des progrès peuvent être accomplis, en lien avec le Conseil européen de l'innovation ainsi que, le cas échéant, avec les services chargés de la gestion du fonds européen de défense.

Encore faut-il noter que **les études technologiques les plus amont n'ont pas nécessairement besoin, en Europe, d'être placées sous les auspices de la politique de défense pour être financées**. En effet, leur champ dépasse les seuls enjeux militaires. Rappelons d'ailleurs que si les États-Unis font reposer une part importante de leur effort en la matière sur une agence du *Department of Defense*, cela tient en partie à leur ordre constitutionnel, qui confère au gouvernement fédéral davantage de compétences en la matière que dans d'autres champs de l'action publique. La situation de l'Union européenne est loin d'être la même.

Aussi le soutien à l'innovation, notamment dans le domaine numérique, est-il l'affaire de tous. Les armées doivent en prendre leur juste part dans la mesure de leurs intérêts, sans chercher à répliquer un « modèle » par une sorte de fétichisme – ou de réflexe de « colonie numérique ».

RECOMMANDATIONS

Affermir notre stratégie technologique et industrielle

1. Consolider une stratégique technologique et industrielle claire, assumée et discutée avec le Parlement. Pour ce faire, les rapporteurs proposent de :

   - créer, auprès de la ministre des Armées, un **conseil de prospective technologique et opérationnelle** chargé d'appuyer l'autorité politique dans l'orientation des choix technologiques du ministère en matière d'armement, s'inspirant du rôle tenu en son temps par le centre de prospective et d'évaluation ;

   - charger ce conseil de piloter la rédaction d'un **document de prospective technico-opérationnelle à trente ans**, qui fixe un cap clair aux travaux de prospective des armées et de la DGA ;

   - articuler avec ce plan les **schémas de prospective technico-opérationnelle** pour chaque milieu d'opération et chaque catégorie de systèmes d'armes ;

   - sur cette base, **associer la recherche et l'industrie** à cette stratégie au moyen de **feuilles de routes** technologiques conclues entre la DGA et les principaux acteurs de la BITD.

2. Conduire des études interdisciplinaires afin de fournir une base à la rédaction, le moment venu, d'une **doctrine française concernant les modalités précises de mise en œuvre du principe dit de « l'homme dans la boucle »** de toute décision opérationnelle.

Ces travaux mériteraient d'être menés dans un cadre associant des spécialistes de la prospective technico-opérationnelle, de la recherche en neurosciences et en robotique ainsi qu'en intelligence artificielle, de la R&D dans les applications de ces sciences et de l'éthique. La doctrine pourrait pertinemment distinguer différents niveaux d'autonomie d'un système d'arme ou d'intelligence artificielle, pour établir des règles graduées.

3. **Réserver les usages sensibles à des logiciels « souverains »**. À défaut de logiciel souverain, favoriser le recours à des logiciels libres et à des développements internes. En parallèle, élaborer une stratégie de reconstitution d'une filière industrielle souveraine de composants numériques.

Structurer un écosystème d'innovation

4. Mettre en œuvre les recommandations du rapport de notre collègue Cédric Villani concernant le secteur de la défense et, ce, non seulement pour ce qui concerne l'intelligence artificielle, mais aussi pour d'autres technologies numériques utiles aux armées, comme la robotique, le *big data* ou l'impression 3D. À ce titre :

   - **soutenir la création de « plateformes sectorielles »** partagées entre acteurs de l'innovation pour mettre en commun des informations, des services ou des équipements, notamment des capacités de calcul intensif et en *cloud* ;

   - mettre à la disposition des organismes de recherche et des industriels innovants des **jeux de données exploitables**, c'est-à-dire expurgées d'éléments classifiés et annotées autant que possible ;

   - favoriser la conduite d'**expérimentations** par les acteurs français de l'innovation, tant par un accès facilité à des installations d'expérimentation **en situation réelle** que par des mesures d'**assouplissement des contraintes administratives**.

L'*Innovation Défense Lab*, une fois constitué en tête de réseau des différents « labs », peut constituer le fer de lance du ministère dans ces actions.

5. Resserrer les liens entre la recherche, l'industrie, l'enseignement militaire, la DGA et les armées, ce qui passe par :

   - des **liens étroits entre l'enseignement militaire supérieur et les** chaires spécialisées dans différentes disciplines intéressant les armées et l'industrie de défense ;

   - **un effort accru de recherches amont dans le secteur dit de la *deep tech***, c'est-à-dire à haut degré de risque, sans chercher à dupliquer la DARPA mais en s'inspirant de ses méthodes de conduite de projet dans le fonctionnement de l'Agence de l'innovation de défense ;

   - une **association plus étroite des industriels français avec des organismes de recherche tel l'INRIA** ;

   - une **consolidation des différents « labs »**, qui gagneront à être mis en réseau par l'*Innovation Défense Lab* et, *via* l'Agence de l'innovation de défense, articulés avec le fonds Définvest pour, le cas échéant, accompagner la croissance des *start-up* ainsi repérées ;

   - un **recours plus fréquent aux « défis »**, ce qui suppose un financement pour leurs participants ainsi qu'un soutien en ingénierie contractuelle pour les services acquéreurs ;

- un renforcement des moyens pratiques de **soutien à l'innovation participative**, sous l'égide de l'Agence de l'innovation de défense ;

6. Lutter contre l'aversion au risque dans les pratiques des administrations, ce qui implique de promouvoir une **culture de l'expérimentation et de l'acceptation de l'échec** en matière d'innovation technologique.

7. Déconcentrer une part des moyens de soutien à l'innovation, par exemple en **confiant aux chefs de corps et commandants de base des crédits destinés à l'expérimentation d'innovations technologiques**, moyennant un dispositif efficace de suivi central des initiatives et de partage de leurs résultats.

8. Dans la lignée du « Pacte défense–PME », **consolider les instruments financiers de soutien à l'innovation visant principalement les *start-up* et autres PME**, afin par exemple de pouvoir financer des *start-up* pour un montant excédant celui de leur chiffre d'affaires, et de rendre les applications purement militaires éligibles à un dispositif comme RAPID.

Réformer les procédures d'acquisition du ministère des Armées

9. Procéder à une réécriture de « la 1516 » de façon à distinguer :

   - **un corpus court de règles et de méthodes communes** à l'ensemble des programmes d'armement ;

   - des **règles de procédure différenciées en fonction :**

     - d'une part, **de la complexité et le coût des programmes**, de façon à alléger les procédures (et donc réduire les délais) pour les programmes les plus simples ;

     - d'autre part, **de la nature des programmes**, de façon à traiter différemment, par exemple, l'acquisition d'un véhicule et celle d'un système d'information.

10. Dynamiser la pratique de la contractualisation et, à ce titre :

    - **promouvoir le recours à des procédures dérogatoires**, telles que le **partenariat d'innovation** ou le **dialogue compétitif**, par des mesures de sécurisation juridique propres à lever les réticences des acheteurs ;

    - inviter la DGA à **contractualiser plus fréquemment avec les *start-up* et autres PME**, soit directement soit à travers un consortium ;

    - sans complexe, **orienter la commande publique** vers des acteurs français ou européen du numérique afin de soutenir la croissance de

« champions numériques » et la constitution d'une offre souveraine pour répondre aux besoins des armées ;

- créer, auprès de l'*Innovation Défense Lab* ainsi que des acheteurs du ministère, des **cellules d'appui expert à la contractualisation** afin de favoriser le recours à des procédures innovantes ou à des fournisseurs autres que les partenaires habituels du ministère.

Créer les conditions d'une exploitation optimale des données

11. Investir dans un **plan de réduction de la fracture numérique** au sein du ministère des Armées, couvrant l'extension de la couverture de ses emprises en accès à internet, le déploiement d'une identité numérique pour tous les personnels, et la mise en ligne d'applications « du quotidien » sur internet aussi souvent que possible, et à défaut sur l'extranet du ministère.

12. Pourvoir au **financement de l'industrialisation des projets de transformation digitale expérimentés avec succès**.

13. **Établir des règles de standardisation et de partage des données** produites dans le cadre de l'activité du ministère des Armées, notamment pour le maintien en condition opérationnelle de ses équipements.

14. Soutenir le développement des technologies de ***cloud computing*** et accompagner la montée en puissance d'un ou plusieurs **opérateurs français** et privilégier la localisation sur le territoire national des infrastructures de stockage et de traitement des données d'intérêt stratégique.

Préparer le combat numérisé de demain

15. Développer des systèmes d'intelligence artificielle à même d'exploiter les données et de fournir à l'homme les informations pertinentes pour prendre rapidement ses décisions sur le champ de bataille, tout en garantissant **l'étanchéité entre les algorithmes d'intelligence artificielle et les systèmes de commande des armes** offensives les plus destructrices.

16. Lancer des études visant à **rendre les systèmes d'intelligence artificielle capables de fournir des justifications de leurs propres résultats**, conditions pour que les applications d'intelligence artificielle puissent être reconnues opérationnelles et soient effectivement adoptées par les forces.

17. Établir, dans un cadre doctrinal d'ensemble, des **normes de cybersécurité du quotidien** prévoyant notamment :

    - une **étude systématique, même rapide, de la cybersécurité de tous les équipements utilisés** au sein des armées, de façon à ce que la doctrine en règle l'emploi de façon sûre ;

- des **règles d'emport et d'usage par les militaires de leurs équipements numériques personnels** ;

- des **compétences de « cyber-hygiène » à valider** par les militaires à l'instruction et dans la formation continue.

18. Accroître l'effectif de **spécialistes du numérique** en promouvant la **réserve opérationnelle** parmi les professionnels du secteur civil et **en développant ces formations** à tous les niveaux : enseignement supérieur « civil », écoles militaires, enseignement militaire supérieur.

19. Ne jamais négliger les **capacités de fonctionnement « en mode dégradé »** des équipements modernes ainsi que la formation des personnels aux opérations « en mode dégradé ». Établir un **plan général de fonctionnement « en mode dégradé »** de l'ensemble des réseaux du ministère des Armées.

20. Conduire des études sur l'intérêt de **capacités d'action cybernétique offensive déconcentrées** qui constitueraient des alternatives aux moyens cinétiques, par exemple à bord des principaux bâtiments de la flotte.

21. **Intensifier les recherches dans l'informatique quantique**, pour préparer des capacités de cryptanalyse, des compétences en cryptographie quantique et des moyens de cryptographie post-quantique.

Utiliser l'échelle européenne comme levier de reconquête d'autonomie stratégique

22. Pour éviter l'enfermement dans certains standards technologiques, promouvoir l'établissement de **normes européennes de cybersécurité et d'interopérabilité** des composants et équipements numériques.

23. Soutenir la **mutualisation européenne des capacités de calcul intensif** et la localisation en France de supercalculateurs, à commencer par l'un des deux calculateurs exaflopiques que financera l'Union européenne.

24. Prendre une part active dans les programmes européens visant à développer des **capacités industrielles européennes dans le secteur des composants**, notamment des processeurs.

25. Promouvoir l'utilisation de la **force de frappe financière et technologique européenne en faveur des recherches de *deep tech***, que ce soit dans le cadre des instruments naissants – comme le fonds européen de défense – ou d'une « DARPA à l'européenne ».

TRAVAUX DE LA COMMISSION

La commission procède à l'examen du rapport de la mission d'information sur les enjeux de la numérisation des armées au cours de sa réunion du mercredi 30 mai 2018.

M. le président Jean-Jacques Bridey. Nous allons procéder à l'examen, ouvert à la presse, du rapport d'information sur les enjeux de la numérisation des armées.

M. Thomas Gassilloud, rapporteur. Nous voici arrivés au terme des travaux de la mission d'information sur les enjeux de la numérisation des armées que vous nous avez confiée le 22 novembre, jour où la commission s'était réunie pour étudier le remplacement du logiciel Louvois. Je dois dire que ces travaux ont été intenses, car le sujet est vaste. Nous avons entendu, dans nos auditions à Paris, une soixantaine de personnalités de tous horizons : opérationnels, ingénieurs de l'armement, grands industriels comme *start-up* et autres PME, chercheurs de toutes disciplines. Nous sommes allés à la rencontre des forces, comme au 12e régiment de cuirassiers ou, hier encore, au 1er régiment d'hélicoptères de combat. Nous nous sommes également attachés à étudier les enjeux de numérisation des forces à l'occasion de nos autres déplacements, hors du cadre de la mission, comme par exemple lorsque j'ai passé le 31 décembre 2017 à Tessalit, au Mali, où la ministre des Armées avait invité quelques-uns d'entre nous. Nous sommes allés rencontrer aussi bien des *start-up* que les chercheurs de nos grands groupes dans leurs laboratoires. Nous avons aussi tenu à participer à différents colloques, par exemple dans le cadre de l'université permanente de la défense ou au forum international de la cybersécurité à Lille. Enfin, nous avons tenu, en dépit de délais serrés, à nous rendre aussi aux États-Unis pour y rencontrer les autorités civiles et militaires compétentes. Bref, nous nous sommes attachés à ce qu'il n'y ait pas d'angle mort dans l'étude de ce phénomène, la révolution numérique, qui bouleverse non seulement nos équipements, mais même dans nos modes de vie.

M. Olivier Becht, rapporteur. Cette révolution numérique a en effet des implications aussi importantes que celles, en leur temps, de l'invention de la poudre ou de la bombe atomique ; selon l'expression consacrée, elle a des conséquences tous azimuts, et particulièrement profondes. Comme vous avez constitué, en parallèle à notre mission d'information, une autre mission consacrée à la cyberdéfense, celle de nos collègues Alexandra Valetta–Ardisson et Bastien Lachaud, nous nous sommes bien sûr interdit de marcher sur les plates-bandes de nos collègues. Nos deux rapports seront sans aucun doute complémentaires. La frontière entre les deux sujets n'est cependant pas étanche ; il serait par exemple bien périlleux de former un avis sur la numérisation de nos armes sans se demander si ces systèmes sont bien sécurisés. Que nos collègues ne nous tiennent donc pas rigueur si, de façon incidente, nous en venons à citer le mot de cyberdéfense.

Nous avons abordé notre vaste sujet d'investigation en quatre temps. D'abord, nous avons dressé un état des lieux de la numérisation de nos armées au sein de la nouvelle programmation militaire.

M. Thomas Gassilloud, rapporteur. Ensuite, nous nous sommes attachés à étudier comment les armements, les ressources humaines et les modes de fonctionnement de nos armées doivent évoluer pour relever le défi des ruptures technologiques envisageables à

moyen terme. C'est à ce titre que nous vous avons soumis des amendements au projet de LPM, et nous nous félicitons d'ailleurs que le Sénat n'ait pas modifié ces dispositions.

M. Olivier Becht, rapporteur. Nous nous sommes ensuite attachés à étudier le revers de la médaille, si j'ose dire, c'est-à-dire les vulnérabilités que crée la numérisation.

M. Thomas Gassilloud, rapporteur. Enfin, sans attendre la récente prise de conscience de l'opinion quant à certaines pratiques de ce que l'on appelle les GAFA – Google, Apple, Facebook et Amazon –, nous avons tenu à mettre en exergue les enjeux de souveraineté qui s'attachent aux technologies numériques, véritables outils de puissance.

M. Olivier Becht, rapporteur. Commençons par le constat, le diagnostic, du niveau de numérisation de nos armées. Ce constat n'est pas binaire. Vous pourrez en lire le détail dans notre rapport, mais pour décrire schématiquement les choses suivant la *summa divisio* « organique / opérationnel », on peut dire que la France n'a pas à rougir du niveau d'intégration du numérique à ses armes, mais que la numérisation est moins avancée dans le fonctionnement courant des armées.

En effet, s'agissant de nos systèmes d'armes, les armées font du numérique depuis plusieurs décennies comme M. Jourdain de la prose. Nos frégates multi-missions et nos futures frégates de taille intermédiaire sont déjà des systèmes numérisés. Dans le milieu aérien, nous ne voyons pas de retard majeur, grâce à la démarche incrémentale retenue par exemple pour le Rafale, dont on programme aujourd'hui le standard F4. Schématiquement, de telles plateformes sont conçues d'ores et déjà comme un ordinateur autour duquel on construit un bateau ou un avion. L'armée la plus rustique en apparence est peut-être l'armée de terre ; mais il ne faut pas oublier qu'elle s'est engagée au tournant des années 2000 dans la numérisation de l'espace de bataille (NEB). Reconnaissons-le : pour de jeunes recrues qui ont peu ou prou l'âge de la NEB, certains de ces matériels ont presque un côté rétrofuturiste... Mais c'est bien sur la NEB que le programme SCORPION fait fond, et je crois qu'en matière de combat collaboratif info-valorisé, avec SCORPION, la France a même une longueur d'avance, reconnue même à Washington.

Les équipements supposent des transmissions et, là encore, il faut reconnaître que nos armées ne sont pas surclassées, que ce soit en matière de radio logicielle ou de télécommunications spatiales protégées. Et quand nos armées ont dû faire face à des besoins opérationnels urgents, elles ont su y répondre. Je pense au système Auxylium de télécommunication sur le territoire national, que nous avons étudié en procédant à l'audition de son inventeur.

De même, les capteurs du renseignement sont à jour. Enfin, ajoutons que notre base industrielle et technologique de défense a su s'approprier très tôt les technologies numériques, tant pour son propre fonctionnement que pour les intégrer à nos armes.

M. Thomas Gassilloud, rapporteur. L'état des lieux est en revanche plus mitigé s'agissant des fonctions organiques de nos armées. Il suffit pour s'en convaincre de se rappeler que vous nous avez confié cette mission le même jour que l'audition de la responsable du programme Source Solde, qui doit réparer les pots cassés de Louvois…

Au-delà même de ce grave échec, dont notre rapport s'attache d'ailleurs à tirer les leçons, nous avons étudié le paysage des 650 applications numériques du champ organique – sur les 1 600 applications au total qu'opère le ministère selon son directeur général des systèmes d'information et de communication. Il en ressort que ce paysage est constitué de systèmes hétérogènes, de générations si différentes que leur interconnexion n'est pas

toujours fiable. C'est à la nécessité de gérer cet héritage informatique que tient l'enjeu de ce que l'on appelle l'urbanisation des systèmes d'information, c'est-à-dire l'articulation des systèmes entre eux, chantier dans lequel il reste beaucoup à faire. Si les armées sont déjà largement numérisées dans le champ opérationnel, où tout est déterminé par les nécessités du combat, elles ont bien davantage de marges de progression dans la numérisation de leurs fonctions organiques, dans lesquelles ne pèsent pas les contraintes de la concurrence.

Il apparaît aussi que, dans ce domaine, les armées ont clairement des marges de progression dans trois séries de fonctions.

Primo, les relations du ministère avec ses administrés, sur le mode de la « relation client ». C'est dans ce domaine que les usages civils du numérique sont pourtant les plus aisément transposables. Aujourd'hui, nos soldats ont plus de liens numériques avec la FNAC ou Amazon qu'avec leur employeur. Il serait fâcheux que ce soit Google ou LinkedIn, sans parler de Facebook, qui en sache plus que les armées sur leurs propres soldats. En plus d'évidentes questions de sécurité, il faut relever le décalage entre la vie numérique du ministère et les pratiques sociales de soldats qui, nés à la fin des années 1990, sont des *digital natives* qui ont grandi avec le numérique.

M. Olivier Becht, rapporteur. *Secundo*, contrairement aux organisations civiles, le ministère ne paraît pas avoir fait évoluer son organisation de façon à tirer profit de la numérisation. Sans céder aux modes du *management*, qui n'ont pas toute leur pertinence dans les armées, retenons que les spécialistes de la chose, comme le général américain Stanley McChrystal, montrent qu'avec le numérique, l'organisation administrative et hiérarchique peut et doit évoluer. Schématiquement, l'heure est aux organisations moins pyramidales et à la circulation de l'information. Certes, l'organisation des armées a beaucoup évolué ces dernières années – peut être trop –, par exemple avec les bases de défense. Mais ces réformes avaient plutôt pour but de réduire les effectifs, parfois à tout prix, que de moderniser l'institution avec le numérique.

M. Thomas Gassilloud, rapporteur. *Tertio*, et c'est peut-être le plus important, les difficultés actuelles de la chaîne de maintien en condition opérationnelle tiennent en partie à un sous-investissement dans sa modernisation, notamment par le numérique. Nous avons pu constater encore hier, au 1er régiment d'hélicoptères de combat, le faible niveau de disponibilité opérationnelle des hélicoptères. Si l'on observe par exemple la maintenance aéronautique civile, elle repose sur des procédures très numérisées, qui permettent d'optimiser l'emploi et la maintenance des matériels. Maintenance prédictive, fluidification des procédures, gestion des stocks, etc. ; les possibilités sont importantes, et les armées ne les exploitent pas encore assez.

Voilà un rapide état des lieux de la numérisation des armées aujourd'hui, qui fait apparaître davantage de points forts en matière opérationnelle qu'organique. Il y a beaucoup à faire dans le grand chantier de transformation numérique engagé par le ministère. Nous en avons discuté lors de l'examen du projet de LPM, et notre commission pourrait s'attacher à le suivre, par exemple en recevant le nouveau directeur général du numérique.

Mais si, globalement, la France n'a pas à rougir, mais elle ne peut pas non plus s'endormir sur ses lauriers, car les ruptures technologiques à venir constituent des défis majeurs pour nos armées.

M. Olivier Becht, rapporteur. En effet, il faut bien mesurer que la révolution numérique ne fait que commencer : c'est une course dans laquelle le France devra tenir son rang, car les nouveaux défis qu'elle crée appellent des investissements capacitaires

nouveaux, parfois extraordinaires, sous peine de déclassement. Nous nous sommes attachés à étudier les ruptures technologiques envisageables et leurs implications capacitaires. Nous n'avons pas la prétention de jouer aux oracles technologiques. Mais nous observons un consensus autour de certaines ruptures technologiques sur plusieurs fronts.

Prenons par exemple le *big data* : ses progrès sont aussi prometteurs pour le renseignement que pour le maintien en condition opérationnelle ou d'autres fonctions organiques, et le déluge d'informations qui caractérise la révolution numérique ne peut être maîtrisé que par ces techniques.

M. Thomas Gassilloud, rapporteur. Prenons aussi l'exemple de la fabrication additive, également appelée impression 3D. Ce pourrait être une quatrième révolution industrielle, qui intéresse notre industrie mais aussi nos armées, directement, car elle peut révolutionner leur logistique en opérations. J'ai pu le mesurer la semaine dernière lors de mon déplacement en République centrafricaine : le sous-groupement tactique interarmes que nous y entretenons est contraint d'acheminer et d'entreposer sur place nombre de pièces de rechanges différentes, au point que cela constitue un véritable montage de ferraille. Ce poids logistique pourrait être considérablement allégé si la force déployée pouvait créer les pièces de rechange dont elle a besoin par des moyens de fabrication additive. Les *Marines* américains, forts de leur retour d'expérience d'Irak, fondent en la matière de grands espoirs sur cette technologie. Schématiquement, l'acquisition d'un équipement ne serait plus assortie de la commande d'un nombre important de pièces de rechange, mais de la livraison des plans permettant de fabriquer celles-ci au moyen d'imprimantes 3D.

Autre innovation de rupture à venir : la course au calcul intensif. Les capacités des supercalculateurs augmentent et permettent de nouvelles applications, notamment en matière de simulation des phénomènes physiques, d'aide à la décision et d'optimisation.

M. Olivier Becht, rapporteur. Nous arrivons effectivement à un moment historique de croisement entre calcul intensif, *big data* et intelligence artificielle. En effet, la multiplication des capteurs, sur les équipements ou sur les hommes, produit un volume considérable de données. L'intelligence artificielle deviendra rapidement indispensable pour trier ces données dans des systèmes de *big data*, afin de présenter aux hommes les seules données utiles pour mûrir leurs décisions.

M. Thomas Gassilloud, rapporteur. On passe en quelque sorte du brouillard de la guerre, situation dans laquelle le soldat manque d'information, au déluge d'information, où les données sont surabondantes. Il s'agit donc de traiter les masses de données et valoriser les informations que l'on en tire en vue d'une décision appropriée. Ainsi, appliquée à des outils de *Command and Control*, l'intelligence artificielle doit permettre de traiter, dans un temps extrêmement bref, les masses colossales de données issues des capteurs, pour soumettre à la décision de l'homme des options optimisées. La guerre de demain pourrait être une guerre d'algorithmes.

L'intelligence artificielle aura un rôle crucial à jouer dans un autre champ de ruptures technologiques : les systèmes autonomes. Drones et robots font leur entrée sur le champ de bataille. Ils sont amenés, qu'on le souhaite ou non, à y prendre une place croissance, au point que certains chercheurs parlent de « robolution ».

M. Olivier Becht, rapporteur. Autre rupture intéressant les armées : l'informatique quantique. Lorsque l'on parle de quantique, on a parfois l'impression de parler de science-fiction… Je ne prétends pas donner ici des explications scientifiques très savantes, mais le principe est le suivant : alors qu'un ordinateur classique fonctionne avec

des bits, ayant de façon binaire une valeur soit d'un, soit de zéro, l'informatique quantique fonctionne avec des qbits susceptibles d'avoir deux valeurs en même temps, comme superposées. Ainsi, alors qu'un ordinateur classique doit réaliser une opération pour chaque valeur qu'il donne, un ordinateur quantique donnerait, en une seule opération de calcul, toutes les valeurs possibles. Cela conduirait à accroître de façon exponentielle la capacité de calcul de l'informatique. Aujourd'hui, l'ordinateur le plus rapide opère environ cent millions de milliards d'opérations par seconde, alors qu'un ordinateur quantique n'aurait quasiment aucune limite. Mais, me direz-vous, quand sera opérée cette rupture technologique ? L'horizon s'approche : on le mesurait en décennies il y a encore quelques années ; aujourd'hui, les Américains l'estiment à cinq ans, et les Japonais de Hitachi sont plus optimistes encore, évoquant un à deux ans. La société canadienne D-Wave commercialise déjà une puce quantique, et la NASA comme Google possèdent déjà des applications quantiques. Une autre chose est certaine : si une telle machine fonctionne, elle bouleversera nos chiffrements. En effet, une puissance de calcul infinie permet de tester en quelques secondes une infinité de combinaisons possibles d'un code. La cryptographie est donc à réinventer, sans attendre que la première puissance à posséder un ordinateur quantique puisse mettre à bas nos défenses cryptographiques.

Nous nous sommes aussi intéressés aux ruptures qui pourraient naître de la convergence, à l'œuvre aujourd'hui, entre neurosciences et numérique. C'est un sujet moins connu, qui relevait de la science-fiction il y a quelques années encore. C'est aujourd'hui un champ de recherches qui enregistre des avancées. Nous nous sommes fait présenter par la DARPA les programmes de recherche RAM et RAM-Replay, qui visent à extraire, restaurer et réimplanter des souvenirs d'un cerveau humain. Autre exemple : les progrès en matière de casques encéphalographiques permettent de transmettre de données par la pensée *via* un casque à électrodes. Ainsi, on peut aujourd'hui contrôler un avion de chasse par la pensée… Certaines expérimentations visent à contrôler des émotions, par exemple pour réduire la peur ou exalter le courage. Facebook annonce pour 2019 la création de casques neurocérébraux permettant de communiquer par la pensée sur le réseau. Les applications imaginables de ces technologies sont vertigineuses, et parfois effrayantes. Elles ne conduisent pas seulement à l'homme dit augmenté, mais ouvriraient la voie à l'homme contrôlé ; l'existence, un jour, de moyens techniques permettant de *hacker* un cerveau humain n'est pas à exclure.

M. Thomas Gassilloud, rapporteur. Nous n'avons pas pour ambition de vous effrayer, chers collègues, par ces perspectives ! (*Sourires*).

Parmi les autres domaines dans lesquels des ruptures technologiques pourraient intéresser les armées, il faut citer aussi l'internet des objets.

L'ensemble de ces ruptures numériques nous semble avoir une conséquence majeure sur l'architecture même de nos armes. En effet, jusqu'à présent, nous concevons un système d'armes comme une plateforme unique, mais désormais, ce sont des systèmes de systèmes qu'il nous faut imaginer.

M. Olivier Becht, rapporteur. Permettez-moi de rappeler en quelques mots ce que l'on entend par « système de systèmes ». Nous vous disions tout à l'heure que, de façon très schématique, on conçoit aujourd'hui une plateforme comme un puissant ordinateur autour duquel on construit un avion, un bateau ou un blindé. Avec les avancées de la technologie numérique, c'est désormais autour d'un réseau que l'on construira plusieurs plateformes, dont l'ensemble des outils de combat – capteurs, leurres et moyens de riposte – seront interconnectés en permanence dans une sorte de *cloud* mettant en œuvre de puissantes capacités de calcul et des dispositifs d'intelligence artificielle pour traiter les données et présenter à l'homme les informations les plus pertinentes. Avec les progrès des technologies

numériques, la supériorité opérationnelle ira à celui qui traitera l'information le plus rapidement ; c'est tout l'enjeu de l'architecture de ces systèmes de systèmes.

Elle a vocation à s'imposer dans tous les milieux d'opérations, où les équipements de demain sont appelés à être les outils du combat collaboratif. Tel est par exemple le cas dans la bulle de combat aéroterrestre avec le programme SCORPION, tel est aussi l'enjeu du système de combat aérien futur, et la même logique est à l'œuvre en matière d'armement naval.

M. Thomas Gassilloud, rapporteur. Je n'évoquerai que rapidement l'importance d'autant plus cruciale que prendront les transmissions et les dispositifs de partage d'information dans ces systèmes de systèmes. En la matière, l'avenir paraît être au déploiement de *clouds* de combat rassemblant, traitant et mettant en réseau les données produites et utilisées par chaque composante de ces systèmes.

M. Olivier Becht, rapporteur. Toutes ces perspectives nous conduisent à nous interroger sur les moyens de maintenir l'homme « dans la boucle » de décisions, dans la guerre numérisée. Notre conviction est qu'en tout état de cause, l'homme doit rester dans cette boucle. Cela n'empêche pas d'exploiter les avancées technologiques. En effet, tout robot n'est pas nécessairement un robot tueur, et comme l'a bien montré le récent rapport de notre collègue Cédric Villani sur l'intelligence artificielle, on ne pourra pas faire sans cette technologie.

La question est donc de savoir comment contrôler l'intelligence artificielle. Cela passe notamment par des développements visant à rendre celle-ci capable de justifier ses résultats. Pour se convaincre de ce que l'on ne peut pas s'y fier sans contrôle, il suffit de se rappeler, par exemple, que le robot de Microsoft doté d'intelligence artificielle, appelé Tay, est devenu très rapidement néonazi. De même, en 2016, deux intelligences artificielles développées dans le cadre du projet *Google Brain* ont inventé, en quelques semaines, un langage nouveau, indéchiffrable par l'homme. Certes, l'intelligence artificielle n'a pas atteint pour l'heure le stade de la singularité, c'est-à-dire celui de la conscience réflexive de soi. Mais c'est dès à présent qu'il faut entamer une réflexion sur le contrôle de l'intelligence artificielle et, par prudence, rendre étanche les réseaux accessibles à des systèmes d'intelligence artificielle et ceux qui commandent des armes de destruction, *a fortiori* des armes de destruction massive.

M. Thomas Gassilloud, rapporteur. Voilà pour les ruptures technologiques à venir dans le champ opérationnel. Dans le champ organique, ces ruptures sont également prometteuses de gains d'efficience. Leurs applications civiles sont bien connues, et notre rapport présente nombre d'expérimentations de terrain, consistant à numériser par exemple les livrets de tir des soldats au 12e régiment de cuirassier. Dans ce cas, la numérisation des procédures a permis de réduire largement la durée des procédures de risque de scorie dans les multiples recopies d'informations. Toutefois, pour progresser dans la numérisation, imaginer sans cesse de nouveaux usages et gagner ainsi en efficience, deux conditions nous paraissent requises.

Première condition : réduire la « fracture numérique » dans les armées qui, sans cela, se privent d'innovations utiles. Un exemple : de nos jours, quelle organisation de 1 000 personnels n'aurait pas la fibre optique ? On peut se retrouver dans une situation où une application numérique est disponible et répond à un besoin, mais où elle ne peut pas être déployée et exploitée pleinement faute de débit suffisant… Il faut donc investir dans des infrastructures numériques de base, c'est-à-dire étendre la couverture des emprises militaires en accès à internet à haut débit, notamment par fibre optique, pour permettre le

développement de nouveaux usages professionnels du numérique ainsi que contribuer à fidéliser les soldats, habitués à utiliser le numérique pour des usages personnels.

Autre exemple : seul un tiers des militaires de l'armée de terre possède une adresse d'email professionnelle. Certains objecteront : mais à quoi bon, s'ils ont fonctionné ainsi jusqu'à présent ? Je crois pourtant qu'un système de messagerie professionnelle constitue une base indispensable, tant pour développer de nouveaux usages que pour cultiver une identité professionnelle.

Seconde condition, c'est toute une « culture de la donnée » qu'il reste à promouvoir. Les armées sont traditionnellement très frileuses envers la circulation de l'information, même non classifiée, alors que dans l'économie numérique, c'est au contraire la circulation des données qui crée de la valeur. Il en va de même dans les armées, surtout dans le champ organique. Une meilleure exploitation des données permettrait par exemple de développer des mécanismes de maintenance prédictive : si l'on observe que telle ou telle pièce a besoin d'être remplacée en moyenne après un temps ou un type d'activité précis, on peut anticiper les commandes et optimiser ainsi la logistique afférente.

M. Olivier Becht, rapporteur. Dans l'opérationnel comme dans l'organique, l'innovation numérique suppose *in fine* de s'appuyer sur un écosystème agile de recherche, d'expérimentation, de développement et d'acquisition d'équipements, capable de faire fructifier les atouts que nous avons. Nous n'avons certes pas les GAFA ou leur équivalent chinois ; mais Israël y arrive, pourquoi pas nous, Français, et *a fortiori* Européens ? Le rapport de notre collègue Cédric Villani sur l'intelligence artificielle va d'ailleurs dans le même sens.

C'est pour affermir une stratégie nationale de développement d'un tel écosystème nous préconisons de recréer, autour de la ministre, un organisme jouant le rôle tenu par le centre de prospective et d'évaluation à l'époque de la construction de notre outil de dissuasion. Cet organisme serait chargé d'élaborer un plan d'orientation des recherches technologiques, à l'instar de ce que le plan prospectif à trente ans était censé le faire, pour fixer des orientations aux travaux technologiques de la DGA. Il est en effet nécessaire de reprendre la main, et ce n'est pas un nostalgique du Gosplan qui vous le dit !

M. Thomas Gassilloud, rapporteur. Pour consolider notre écosystème d'innovation numérique, la France doit resserrer encore les liens entre les armées, la recherche, la R&D, les *start-up* et les grands groupes intégrateurs de technologies.

Aux États-Unis, cet écosystème est très soutenu par la *Defense Advanced research Projects Agency*, la DARPA, qui finance des projets de recherche et développement qui n'ont pas d'application immédiate envisagée dans un programme d'armement, ce qui autorise les laboratoires à conduire des recherches sur des objets technologiques dont on ignore encore l'application. En France, la direction générale de l'armement (DGA) dépense 85 millions d'euros par an « en mode DARPA », contre trois milliards de dollars par an pour la DARPA. L'équivalent serait assurément hors de notre portée, mais on peut certainement faire mieux que 85 millions d'euros.

M. Olivier Becht, rapporteur. En réalité, qu'est-ce qui fait la force de la DARPA ? Nous distinguons trois facteurs. D'abord, sa force de frappe financière, qui est considérable. Ensuite, l'écosystème de recherche et de R&D sur lequel elle s'appuie, qui constitue un véritable complexe militaro-numérique. Enfin, ses méthodes de travail.

On l'a dit, la DGA peut certainement investir davantage dans la *deep tech*, mais elle ne rivalisera avec la DARPA sur ce plan. Quant à l'offre de recherche et de R&D, le réseau universitaire américain n'a guère d'équivalent dans le monde, non pas du point de vue qualitatif, car nos chercheurs soutiennent parfaitement la comparaison, mais du point de vue quantitatif.

En revanche, s'il y a une chose pour laquelle la France peut s'inspirer de la DARPA, ce sont ses méthodes de conduite de projet, notamment l'acceptation de l'échec. Les Américains sont capables d'accepter que plusieurs dizaines de millions de dollars aient été dépensés sans que cela débouche sur le développement d'un équipement. Chez nous, dépenser de telles sommes en R&D sans débouché capacitaire créerait un scandale administratif, financier et probablement politique. C'est là une révolution culturelle en matière de recherche, et c'est à nos yeux une voie dans laquelle la DGA devrait s'engager.

M. Thomas Gassilloud, rapporteur. L'innovation d'usage mérite elle aussi d'être favorisée. On entend par là l'appropriation d'une technologie développée pour d'autres usages, notamment civils. Nous avons été parmi les premiers parlementaires étrangers à visiter le service du Pentagone spécialisé en la matière, appelé *Strategic Capabilities Office*. Un meilleur soutien à l'innovation d'usage nous apparaît comme un des enjeux majeurs de la création de l'Agence de l'innovation de défense.

Dans le même ordre d'idées, nous trouvons très positifs les « défis », qui consistent pour les armées à inviter tous types d'innovateurs à proposer des réponses technologiques à un besoin donné. Cette démarche, très adaptée aux pratiques de l'économie numérique, mérite d'être généralisée.

M. Olivier Becht, rapporteur. Pour aller plus loin, nous estimons aussi qu'il faut revoir les rapports entre le ministère, les grands industriels et les *start-up* et autres PME. Leurs relations sont aujourd'hui organisées de façon très pyramidale : le ministère privilégie la contractualisation avec les grands groupes, à charge pour eux de sous-traiter une partie de l'activité aux *start-up* et autres PME. Nous pensons que le ministère devrait davantage contractualiser avec ces *start-up* et ces PME.

Nous pensons aussi qu'il est impératif de revoir l'instruction ministérielle qui règle les procédures d'acquisition et de conduite de programmes d'armement, communément appelée « la 1516 ». Il est tout de même assez paradoxal qu'elle permette de déroger à nombre des règles du droit commun des marchés publics pour des programmes de plusieurs milliards d'euros alors que pour le moindre développement de logiciel à un million d'euros, l'ensemble des procédures classiques s'appliquent. Pour ces marchés publics, ce sont souvent les grands industriels qui sont les mieux placés pour soumettre des offres, or dans l'économie numérique, les plus grands groupes ne sont pas français. Aujourd'hui, cela peut être les GAFA, et demain, leur équivalent chinois. Face à la puissance de feu financière de ces géants, les chances d'une entreprise européenne sont pratiquement nulles. Sauf à ce que l'on mette sur pied un Airbus du numérique, l'État doit donc se donner les moyens de passer des commandes à nos *start-up* et à nos PME.

M. Thomas Gassilloud, rapporteur. Je n'insiste pas sur les investissements à consentir en matière de ressources humaines, dont chacun comprend bien la nécessité, tant pour former des spécialistes du numérique que pour les fidéliser. De même, nous ne nous étendrons pas sur l'intérêt qu'aurait l'État à soutenir notre écosystème de recherche et d'innovation numérique en lui fournissant des capacités de calcul.

Venons-en à ce qui est le revers de la médaille dans la numérisation des armées, à savoir la vulnérabilité des forces aux attaques cybernétiques, qui s'accroît avec leur surface d'exposition numérique. Numériser davantage les armées n'est pas pensable sans efforts de cybersécurité et d'aptitude à opérer en mode dégradé. À cet égard, deux brèves remarques.

D'une part, les vulnérabilités numériques pèsent aussi sur nos adversaires. Dès lors, pourquoi ne pas concevoir nos équipements de façon à permettre au chef tactique d'utiliser soit des armes à effet numérique, soit des armes à effet cinétique ?

M. Olivier Becht, rapporteur. Deuxième remarque brève : l'ordinateur, comme l'ensemble de nos « jouets » informatiques, nous apportent beaucoup, mais c'est lorsqu'ils tombent en panne que l'on prend la mesure de notre dépendance numérique. Aujourd'hui, les armées américaines apprennent aux soldats à s'orienter avec des cartes, sans GPS, et aux marins à naviguer au sextant, sans satellite. Ainsi, il faut non seulement veiller à la résilience de nos équipements numériques, mais aussi à conserver nos aptitudes à opérer en mode dégradé, c'est-à-dire sans moyens numériques, pour le cas où nos matériels informatiques seraient indisponibles.

Nous tenons aussi à rappeler que gagner la bataille technologique ne suffit pas à gagner la guerre. Les conflits récents dans lesquels ont été engagées les armées américaines ont bien montré que gagner la guerre, c'est avant tout gagner la paix, c'est-à-dire acquérir la confiance des populations pour stabiliser les théâtres d'opération, ce que la machine ne suffira jamais à faire. Ne cédons pas à l'*hybris* technologique.

M. Thomas Gassilloud, rapporteur. C'est tout le paradoxe de nos travaux sur le rapport des armées aux nouvelles technologies : il faut à la fois savoir faire avec, pour faire mieux, et savoir faire sans, pour faire en tout état de cause. Jamais l'ascendant technologique n'a suffi à gagner une guerre. Il suffit pour s'en convaincre de se pencher sur l'histoire de la guerre d'Algérie, dans laquelle les troupes françaises étaient dix fois plus nombreuses et dix fois mieux équipées que l'ennemi.

Pour finir cette présentation, nous tenons à souligner les enjeux de souveraineté qui s'attachent à la maîtrise des technologies numériques. Force est de reconnaître que les grandes puissances du numérique sont les États-Unis et la Chine : nous faisons tourner des applications américaines sur des composants chinois. Et les ruptures technologiques à venir risquent d'accroître notre dépendance. Prenez le cas de l'intelligence artificielle : Américains et Chinois investissent massivement ; nous, nettement moins. Or s'il est un secteur qui ne peut pas se satisfaire d'une dépendance technologique, c'est bien la défense. Acquérir des matériels étrangers crée déjà une regrettable dépendance lorsqu'il s'agit d'équipements classiques, et cette dépendance n'est que plus dangereuse s'agissant d'équipements numériques. En effet, non seulement l'importation prive notre industrie d'activité, mais l'usage d'équipements numériques expose en lui-même à tous types de vulnérabilités : mise hors-service, captation de données, ou repérages.

M. Olivier Becht, rapporteur. Il faut ajouter qu'acquérir des équipements numériques à l'étranger a aussi pour effet de tarir l'activité de notre R&D, et donc d'hypothéquer notre potentiel technologique futur. De surcroît, même en intégrant seulement des briques technologiques américaines dans ses productions, un industriel s'expose à des règles extraterritoriales d'autorisation des exportations et réexportations d'armement : on met ainsi notre BITD à la merci d'une politique commerciale américaine qui n'évolue pas dans un sens coopératif.

M. Thomas Gassilloud, rapporteur. Pour toutes ces raisons, nous pensons que la commande publique doit être sans complexe orientée vers le soutien à l'industrie numérique française. Américains ou Chinois ne s'en privent pas. Le secteur de la défense jouit de dérogations au droit de la concurrence ; il convient de les exploiter pleinement.

M. Olivier Becht, rapporteur. Je conclurai en soulignant, sans céder à la tentation d'invoquer toujours l'Europe comme seule issue à nos faiblesses, qu'il y a des choses à faire à l'échelle européenne. La période est propice : le fonds européen de défense vient d'être mis sur pied, les propositions de la commission pour le budget pluriannuel 2021–2027 sont favorables, et il y a des projets pour lesquelles la taille critique, c'est l'Union. Nous pensons à des efforts de normalisation des produits et des composants numériques, au financement de calculateurs exaflopiques, ou au développement d'une filière industrielle souveraine de composants informatiques, comme les processeurs. Et bien sûr, nous n'oublions pas l'idée d'une DARPA européenne, l'initiative JEDI. Quelle que forme que prenne une telle idée, nous sommes convaincus que l'Union pourrait investir davantage dans la *deep tech*.

Voilà, Monsieur le président, mes chers collègues, le résultat de six mois de passionnants travaux.

M. le président. Merci aux rapporteurs. Mes chers collègues, il y a douze questions de députés… mais aucune de députée, Mesdames. Je ne vais donc pas pouvoir alterner comme à mon habitude. *(Exclamations)*. Mais il n'est pas trop tard !

M. M'jid El Guerrab. Nous avons une candidate à ma gauche !

M. le président. Alors levez la main ! Nous allons commencer par Jacques Marilossian…

M. Jacques Marilossian. Merci Monsieur le président. Laissez-moi d'abord remercier nos deux rapporteurs et saluer ce travail. J'ai passé trente-cinq ans dans l'industrie informatique. J'ai proposé une journée de travail chez IBM, non loin d'ici, sur l'informatique quantique, la *blockchain*, le traitement d'information, etc. Je pense que nous aurons l'occasion de nous pencher sur ces sujets. Ma question est simple : après tous vos travaux, quelle vous paraît être la première des priorités en matière de coopération européenne pour améliorer notre autonomie stratégique ?

Mme Sabine Thillaye. Florence Parly a annoncé au mois de mars le lancement d'une agence d'innovation de défense, un peu sur le modèle de la DARPA américaine. Où en sommes-nous au niveau budgétaire et capacitaire et comment cela peut-il s'articuler avec la proposition de notre président d'une agence de recherche de rupture européenne ?

M. Damien Abad. La numérisation des armées a des implications profondes pour le monde de la défense. Je voudrais revenir sur la distinction que vous avez faite entre l'opérationnel et l'organisationnel. En matière de gestion des ressources humaines, comment recruter les profils plus « connectés » dont les armées ont besoin ? Quels types de qualification sont nécessaires ? Quel impact cela aura-t-il sur les chaînes hiérarchiques de commandement ?

Ensuite, vous avez parlé de la culture de la donnée. Ce sera un enjeu central parce qu'il y aura de plus en plus de données à collecter. Mais le revers de la médaille, vous l'avez évoqué, c'est la vulnérabilité.

Enfin, dernier point, sur nos PME. Je partage ce que vous avez dit sur la commande publique. Avez-vous le sentiment qu'au niveau national ou européen, *via* le Fonds européen de la défense, par exemple, nous aurions la possibilité de mobiliser des crédits pour développer l'intelligence artificielle mais aussi aider et accompagner nos PME ?

M. Stéphane Demilly. Le 3 mai dernier, à l'occasion de son 25e anniversaire, le commandement pour les opérations interarmées organisait un forum sur le commandement opérationnel interarmées et la numérisation. L'objectif affiché de cet événement, qui rassemblait des opérationnels, des entrepreneurs et des chercheurs, était d'explorer les évolutions ou les révolutions que les avancées technologiques permettaient d'envisager dans la façon de planifier et de conduire les engagements opérationnels au siècle prochain. Le chef d'état-major des armées, le général François Lecointre, avait déclaré que l'approche globale qui nous est imposée aujourd'hui doit s'accompagner – et c'est, à l'évidence, un facteur de supériorité opérationnelle – d'une capacité d'imagination et de créativité. Il faut pouvoir le faire en s'appuyant sur les nouveaux outils du numérique, comme l'intelligence artificielle. Par la numérisation, il s'agit donc de gagner un temps précieux d'avance, comme le soulignent le général François Lecointre et votre excellent rapport. Pouvez-vous nous dire ce que vous avez pensé de ce forum ? Le commandement des opérations interarmées a constitué un groupe de travail sur la numérisation. Avez-vous eu le temps d'avoir des échanges avec ses membres et pouvez-vous nous en parler ?

M. Joaquim Pueyo. Vous avez parlé de « revers de la médaille ». Il est évident que si un adversaire peut s'approprier des données lui permettant aussi bien de connaître nos forces et nos plans que de modifier ces données, nous courrons un grand risque. Vous a-t-on fait des observations à ce sujet au cours de vos entretiens ? Je suis évidemment favorable à la numérisation, à la condition qu'elle soit très bien sécurisée. Comme je reviens, avec ma collègue, de l'assemblée parlementaire de l'OTAN, il faut que vous sachiez que cela avait été un sujet de discussion au sein de l'OTAN. Avez-vous davantage d'informations sur ces risques ?

Le deuxième enjeu, me semble-t-il, tient à la formation des personnels. Les technologies numériques doivent être mises en œuvre et entretenues par des techniciens hautement qualifiés. Nous aurons des soldats techniciens, dans quelques années. Leur formation sera chronophage. Pourrons-nous répondre à ce défi ? Elle sera, à mes yeux, la clé du succès.

M. Jean-Pierre Cubertafon. Je tiens, comme l'ensemble de mes collègues, à vous féliciter ! On s'attendait à un rapport « moyen »… *(Rires)*

… et il est brillant ! J'ai pu observer au cours de deux déplacements ces dernières semaines tout le potentiel technologique et numérique de nos armées. Je pense que nous disposons de réelles capacités en matière numérique, mais qu'elles ne sont pas encore totalement exploitées. Et je vous rejoins sur deux propos : le virage numérique et l'indispensable évolution de nos armées. J'aurais souhaité vous interroger sur le traitement des *big data* et la manière dont nos soldats pourront s'en servir, et à quelle fin. Il est utile dans le renseignement, évidemment. Mais quelle pourra être leur utilisation dans le cadre de dispositifs de défense ou même sur un théâtre d'opérations ?

M. Alexis Corbière. Encore merci pour la qualité de ce rapport. Il est prévu que l'armée française compte d'ici huit ans 4 000 personnels affectés au domaine de la cyberdéfense. Comparé au nombre de *hackers* américains, russes ou chinois, estimez-vous que ce nombre est suffisant pour faire face à ces enjeux ? Et sinon, quel serait le nombre de personnels requis ? Par ailleurs, il est important que nous puissions garantir notre

indépendance et notre pleine souveraineté. Actuellement, les données des systèmes numériques risquent d'être captées par des puissances étrangères. Que peut faire la France pour garantir la sûreté de son propre matériel et ne doit-elle pas développer son propre modèle de drone pour arrêter d'utiliser le drone *Reaper* fourni par l'industrie américaine ?

M. André Chassaigne. Quelles sont les conséquences de la généralisation du numérique sur l'indépendance et la souveraineté nationale, compte tenu de la volonté de nuisance de certains États, groupes politiques, criminels ou individus aux motivations multiples ? Je m'inquiète de la contradiction que je vois poindre entre, d'une part, l'interdépendance très forte inhérente au développement de ces technologies, et d'autre part, la nécessité de conserver une autonomie stratégique. Quels sont les intérêts vitaux de la France dans ce domaine ?

M. Thomas Gassilloud, rapporteur. Merci pour toutes ces questions. À titre liminaire, comme le président regrettait l'absence de questions de la part de nos collègues députées, je m'aperçois que nous avons peu développé dans le rapport l'enjeu de la mixité. M. Mounir Mahjoubi a également souligné à Lille, au forum international de la cybersécurité, la faible féminisation des entreprises du numérique. Or, on code un logiciel en fonction de l'être que l'on est. Si ce sont des hommes qui codent, ils coderont avec leur personnalité et peut-être que ce ne sera pas représentatif de l'ensemble de la population puisque vous savez que les hommes n'en représentent que la moitié. La faible féminisation dans le domaine du numérique s'ajoute à la faible féminisation dans le domaine de la sécurité et de la défense. Les sujets à l'intersection sont donc très peu féminisés. C'est un vrai problème qui devra sans doute être corrigé avec des politiques de ressources humaines adaptées.

Je vais me concentrer sur les questions relatives aux ressources humaines, laissant mon collègue s'exprimer sur les questions de technologies et de moyens. M. Abad, vous posez la question des profils spécialisés qu'il est parfois difficile de recruter. La réponse standard repose souvent sur les niveaux de salaire et l'externalisation. Ce sont des réponses un peu toutes faites et j'aimerais aller un peu plus loin. À la suite de nos auditions, notamment celle de la direction du renseignement militaire, et je le constatais également dans mon entreprise, il me semble que les jeunes générations ne font pas uniquement leur choix de travailler à tel ou tel endroit en fonction du salaire mais aussi en fonction du sens qu'elles donnent à leur métier. Les armées et les services de renseignement sont très attractifs même s'ils ne proposent pas des grilles de salaire comparables à ce qu'on peut voir dans le privé. Mais cela fonctionne, à condition que la personne donne un sens à ce qu'elle fait et qu'elle soit accompagnée dans ce qu'elle fait. Nous avons eu quelques retours « en *off* » sur le découragement suscité par des délais de validation inhérents aux procédures administratives des armées pour obtenir du petit matériel, comme un ordinateur. Le jeune spécialiste en mesure de venir travailler pour les armées ne supporte pas de devoir attendre un temps considérable pour se voir affecter des ressources. Il faut donner la capacité à ceux qu'on recrute d'exercer correctement leurs missions. C'est un point sur lequel nous devons travailler.

Une question portait sur la manière de concilier la culture de la donnée avec la sécurité informatique. Il faut faire preuve de pragmatisme et évaluer avec suffisamment de finesse en quoi une donnée est sensible. Je vais prendre l'exemple des données qui pourraient être utilisées dans le cadre du maintien en condition opérationnelle prédictif. Le taux de panne des pièces de véhicules militaires est évidemment sensible mais les armées doivent être en mesure de les partager avec les industriels qui, du reste, en ont déjà une idée puisqu'ils font leurs propres tests. Autre exemple : aujourd'hui, un Rafale emmagasine

chaque jour plusieurs dizaines de téraoctets de données, notamment avec ses capteurs optiques. Il enregistre sur des kilomètres des bandes de terrain sur lesquelles il procède à des détections. Ce qui est confidentiel, c'est l'aiguille dans la botte de foin, le petit élément aperçu. Pour autant, c'est l'ensemble de données collectées qui ne sort pas du service qui les a commandées. Or, ces données sont nécessaires pour construire les algorithmes qui, demain, permettront de retrouver cette aiguille dans la botte de foin. L'absence d'accès à ces données nous prive de la matière première permettant de construire l'outil de demain. Il doit donc y avoir un arbitrage entre la protection des données et leur partage, qui permet l'innovation, laquelle est indispensable.

M. Olivier Becht, rapporteur. Je vais répondre à notre collègue Jacques Marilossian sur la priorité en matière de coopération européenne… Malheureusement, vous avez compris que tout se tient dans les technologies numériques, il ne peut y en avoir qu'une. On ne peut ériger en un seul élément de cette chaîne technologique et négliger tout le reste. Il me semble essentiel, cela dit, de garantir notre souveraineté en matière de micro-processeurs au niveau français ou européen. En effet, un micro-processeur peut être « vérolé » sans qu'on puisse le savoir. Les bombes logiques existent déjà aujourd'hui mais demain, vous aurez les bombes logiques intelligentes, celles qui seront capables de ne pas se faire déceler et de changer d'apparence ou d'emplacement au moment où elles seront détectées. En matière de *cloud*, qui permet de stocker la donnée, il nous faut des fermes de serveurs françaises ou européennes, implantées sur notre territoire, pour conserver notre souveraineté. L'intelligence artificielle est naturellement essentielle. Enfin, le quantique est pour moi une priorité car c'est la vitesse du traitement des données qui est en jeu. C'est elle qui fera la différence et permettra de réagir avant que l'adversaire n'engage une frappe.

Quant à l'idée d'une DARPA européenne, autrement dit une agence d'innovation de rupture, en réponse à la question de Sabine Thillaye, je note tout d'abord que la structure promouvant la *Joint European Disruptive Initiative* (JEDI) est une entité privée, associant plusieurs industriels. Au niveau français, il n'est pas exclu de soutenir cette initiative mais une agence de l'innovation de défense est aussi en cours de constitution, pourvue en personnels à la fois par les armées et par la direction générale de l'armement. C'est la raison pour laquelle nous avons insisté dans l'examen de la loi de programmation militaire sur la hausse des crédits en faveur de la recherche amont.

Sur la question de notre collègue Joaquim Pueyo nos vulnérabilités numériques, la question du quantique me paraît fondamentale. J'étais la semaine dernière au Japon, où l'on m'a présenté un disque de la taille de ma main et de l'épaisseur d'un cheveu recelant cinq milliards de transistors qui sont capables de faire cent millions de milliards d'opérations par seconde ! Cela paraît déjà considérable mais demain, le quantique permettra des milliards de milliards de milliards d'opérations par seconde. Les codes actuels seront nécessairement cassés. Cela ne veut pas pour autant dire que nous n'aurons plus de capacité de cryptologie. Simplement, elle doit changer. Par exemple, une grille de code pourrait changer toutes les secondes, pour limiter la portée de la cryptanalyse quantique.

C'est un changement total dans les communications cryptées. S'agissant du drone souverain souhaité par Alexis Corbière, j'indique que c'est exactement ce que nous sommes en train de développer avec le programme de drone EUROMALE. Sur la guerre hybride évoquée par André Chassaigne – vous avez parlé de mafias, de réseaux terroristes voire d'États cachés derrière des réseaux privés – c'est un vrai problème, notamment pour l'attribution d'attaques cyber. Il va falloir sécuriser nos armes pour éviter qu'elles ne se retournent contre nous et sécuriser aussi nos réseaux d'infrastructures civiles, par exemple, celles des réseaux de transport ou d'électricité, qui sont une source de vulnérabilité.

M. Thomas Gassilloud, rapporteur. Je vais répondre rapidement aux dernières questions. Stéphane Demilly, j'ai entendu votre question sur le forum du 5 mai mais je n'y étais pas donc je ne peux pas y répondre. Joaquim Pueyo parlait de la formation. Je constate que les personnes qui sont le mieux formées et qui progressent le plus sont celles qui changent d'entreprise tous les trois ou quatre ans. Ce n'est pas forcément transposable aux armées. La bonne formation des spécialistes repose à mon avis sur leur aptitude à alterner des postes de commandement ou d'état-major et de postes de spécialistes, puisqu'un système a toujours vocation à répondre aux contraintes de terrain. C'est ce que font très bien les gendarmes. Il faut également parler de la formation de l'ensemble des militaires. Si un soldat doit avoir des aptitudes physiques ou des aptitudes au tir, on attend aussi de lui une sorte d'hygiène numérique qui consiste à être conscient, par exemple, que s'il porte une montre connectée pendant une opération spéciale, cette montre peut diffuser sa position. Les chefs tactiques doivent aussi être formés. Je suis convaincu que même sur un champ de bataille ultra-numérisé, ce qui fera la différence au moins pour quelques dizaines d'années encore, ce sera la compétence du chef tactique, au-delà de la technologie dont il dispose.

Jean-Pierre Cubertafon posait la question des apports du *big data*. Si je prends l'exemple de l'armée de terre, SCORPION est une première étape dans l'exploitation de cette technologie. Grâce à l'échange en temps réel des informations, plusieurs capteurs peuvent détecter un tir ennemi et en trouver l'origine grâce à la triangulation. Mais on ne peut pas encore parler de *big data* au sens strict puisque l'information disparaît après avoir été partagée. L'étape suivante, c'est la capacité à stocker toutes les informations relevées sur le champ de bataille pour organiser la meilleure riposte en fonction de situations qu'on aura déjà connues. Cela impose au système de communiquer avec un *data center* pour stocker ces données et les valoriser.

Je souhaiterais remettre tout cela en perspective. Lorsqu'on a produit le VAB dans les années 1970, on pensait qu'on ne le modifierait pas durant trente ans. Or, le VAB a connu des « *patchs* » jusqu'à aujourd'hui. Le Griffon comme le VAB connaîtra dans les années à venir des améliorations, du fait du développement de nouvelles fonctions, pas toutes imaginables aujourd'hui. Par exemple, plutôt que de mettre en danger la vie de soldats dans des véhicules qui risquent de sauter sur des IED, des véhicules autonomes pourraient être placés en ouverture d'un convoi. Les cycles d'évolution technologiques seront très raccourcis.

M. le président. J'ai encore sept questions.

Mme Laurence Trastour-Isnart. La numérisation est un moteur de transformation puissant dans le monde militaire et un outil de prise de décision toujours plus performant. Avez-vous pu évaluer de façon globale l'appropriation de cette technologie émergente par nos militaires ? Avez-vous perçu des réticences ou, au contraire, des attentes ?

M. Jean-Michel Jacques. Je me permets d'ouvrir une petite parenthèse en tant qu'ancien militaire : l'issue de la guerre d'Algérie n'est pas la conséquence d'une défaite militaire mais d'un choix politique délibéré.

Nous avons parlé d'ordinateurs placés au cœur d'avions ou de chars, mais ne pourrions-nous pas imaginer un ordinateur à l'intérieur même d'un homme, c'est-à-dire un homme bionique ?

Lors de votre présentation, vous avez mis en exergue la panne comme principale limite de ces technologies. Nous maintiendrions donc toujours une présence humaine sur nos

champs de bataille afin de pallier cela. En conséquence, doit-on s'attendre un jour à assister à des combats entre hommes et robots ?

M. Yannick Favennec Becot. Selon une note de la compagnie européenne d'intelligence stratégique, en 2016, de nombreuses applications relatives à l'administration et à la gestion sont passées dans le *cloud* privé du ministère de la Défense. Lorsque ladite note a été rédigée, l'usage du *cloud* se limitait à ce travail administratif et n'était pas exploité sur les théâtres d'opération. Pouvez-vous nous dire ce qu'il en est aujourd'hui ? Pouvons-nous imaginer, à moyen terme, que nos forces armées déployées sur le terrain aient la possibilité de toutes se connecter à un « *cloud* tactique » leur permettant d'échanger des informations et d'avoir rapidement accès à une grande quantité d'informations ? Une telle avancée technologique leur octroierait plusieurs avantages substantiels, notamment un accès et un partage de l'information accrus, une meilleure interopérabilité et, enfin, un risque de perte de données amoindri dans le cas de destruction de matériel ou de mort d'un soldat.

Cela pose bien évidemment un certain nombre de questions : comment maintenir un contact réseau permanent entre des troupes éloignées de plusieurs centaines voire milliers de kilomètres ? Comment faire en sorte que les forces demeurent opérationnelles même une fois déconnectées ? Et enfin, comment se prémunir contre l'interception et le vol de données par l'ennemi, qui voudrait, par exemple, s'informer sur la disponibilité de nos munitions ?

M. Charles de la Verpillière. La numérisation crée à la fois des opportunités, en tant que facteur d'efficacité de nos armées, mais aussi des vulnérabilités. Parmi celles-ci, on doit prendre en compte la question de la dépendance technologique. Pourriez-vous revenir sur cet aspect ? Elle peut en effet survenir lorsque nous achetons des systèmes complètement étrangers, notamment américains, mais aussi lorsque nous intégrons des composants américains dans nos systèmes français ou européens. Il s'agit ici d'évoquer la question de la réglementation dite ITAR, pour *International Traffic in Arms Regulation*.

M. Christophe Lejeune. Dans votre exposé, vous avez évoqué le militaire à qui on allait réapprendre à lire une carte et le marin à qui on allait réapprendre à naviguer avec un sextant. En cette année de centenaire de l'armistice de la Première Guerre mondiale, cela me fait penser que, peut-être, les élevages de pigeons voyageurs ont de beaux jours devant eux. (*Rires*)

Compte tenu du développement rapide des technologies numériques à usage dual ou militaire, comment pourraient évoluer les menaces provenant d'État-puissances ou d'ennemis non-étatiques ? D'autre part, dans la situation d'asymétrie des forces que nous connaissons sur les théâtres actuels, quels peuvent être les inconvénients de la numérisation des opérations et des champs de bataille pour nos armées ?

M. Loïc Kervran. Je voudrais revenir sur la menace que peut représenter l'utilisation individuelle des outils numériques par les personnels militaires, que ces outils soient personnels ou fournis par nos armées. L'exemple le plus emblématique et le plus à même d'illustrer cette menace est l'utilisation, par des agents de la DGSE, de l'application Strava, qui permet de suivre les déplacements de l'utilisateur lors de ses courses à pied ou à vélo par géolocalisation. On peut également penser à d'autres actes simples et banals mais porteurs de dangers, comme brancher une clé USB personnelle sur un réseau militaire ou encore envoyer des données par mail vers sa boîte personnelle.

J'aimerais ici aborder la question du niveau de sensibilisation des militaires à ces dangers mais également du niveau d'exigence entretenu par les supérieurs, notamment à travers la prise de sanctions. Je viens personnellement d'une entreprise privée, où le simple

fait d'envoyer un mail comportant des données professionnelles vers une boîte mail personnelle étant passible de licenciement. Aussi, je me demandais s'il existait une telle dimension coercitive dans le domaine militaire compte tenu de l'ampleur de la menace.

M. Jean-Charles Larsonneur. Concernant la question de la souveraineté numérique, force est de constater que nous faisons appel à un grand nombre de prestataires extérieurs : Microsoft pour les armées, Ericsson ou encore TechOne pour la police et les centres d'appels. Aussi, est-il légitime de se demander : avons-nous une véritable politique permettant de faire émerger des champions nationaux ou européens dans ces domaines ? D'autre part, ne devrions-nous pas cibler des domaines d'investissement précis plutôt que de disperser nos ressources de manière moindre entre la cybersécurité, le chiffrement et les logiciels de traitement ?

M. Thomas Gassilloud, rapporteur. Madame Trastour-Isnart, j'ai trouvé les militaires très réceptifs et volontaires concernant ces questions technologiques, et manifestant beaucoup d'attentes. Ils sont bien conscients des opportunités qu'offrent les outils numériques à la fois dans leur usage civil et sur le terrain, face à l'ennemi. D'ailleurs, aujourd'hui, même des ennemis réputés « à faible niveau technologique » utilisent ces outils numériques au quotidien.

Les militaires, eux, y voient surtout un moyen d'optimiser leurs procédures administratives afin d'éviter les saisies multiples dans divers systèmes d'information.

Concernant l'utilisation personnelle de technologies telles que le *smartphone* par des agents du renseignement ou des militaires, il est plus que nécessaire d'avoir conscience des risques induits par le seul service de géolocalisation. On considère que 50 % de la population utilise des téléphones portables fonctionnant sous Android, donc par extrapolation, nous pouvons estimer que cela concerne également la moitié des militaires. Cela implique que Google, qui géolocalise ses utilisateurs en permanence, est en mesure de recomposer l'organigramme de l'armée française. En effet, le logiciel pourrait identifier la fonction voire le grade du militaire selon ses déplacements sur les sites protégés et ses voyages à l'étranger.

Le service de géolocalisation implique donc un certain nombre de risques, et tel est aussi le cas d'autres outils numériques, par exemple la possibilité d'utiliser le *smartphone* d'un individu comme un microphone afin de l'espionner.

On peut donc progresser sur la question de l'hygiène numérique, notamment en faisant prendre conscience à nos soldats que l'utilisation de leurs matériels technologiques implique des dangers. On pourrait également penser à fournir un *smartphone* sécurisé aux personnels habilités à manipuler des données sensibles comme il a été fait dans la gendarmerie. Après en avoir discuté avec l'amiral Arnaud Coustillière, deux choix s'offrent à nous : soit développer une simple application qui serait installée sur les *smartphones* personnels des militaires, soit considérer que le *smartphone* peut réellement être vu comme un équipement militaire, auquel cas nous estimerions collectivement que fournir directement un téléphone portable sécurisé à l'agent est un investissement acceptable.

Il est fort probable que des choix similaires se présentent en ces termes à l'avenir, mais dans un premier temps, l'hygiène numérique est le point fondamental à traiter.

Concernant la question des mesures coercitives contre les militaires imprudents dans le maniement d'outils numériques, la diffusion de contenu protégé sur les réseaux

sociaux a déjà donné lieu à des sanctions dans les armées par le passé. Aussi, je dirais que les chefs militaires sont tout à fait capables de prendre les mesures qui s'imposent.

M. Olivier Becht, rapporteur. M. Jacques, l'utilisation de robots sur le champ de bataille va sans doute se limiter, pour quelques décennies encore, à la conduite de certaines missions, je pense notamment au déminage ou encore au transport de blessés. Pour le reste, l'homme sera *dans* le robot – si l'on considère que les matériels demain, char ou avion par exemple, seront des robots, à savoir des machines embarquant un ordinateur et dotées d'une certaine autonomie –, et en gardera la maîtrise.

Va-t-on vers l'homme augmenté, c'est-à-dire le syncrétisme entre l'homme et la machine ? Très certainement, et on le voit déjà dans un certain nombre d'applications. La guerre des robots sera-t-elle forcément « meilleure » que celle d'aujourd'hui ? C'est une question que je ne trancherai pas maintenant. Davantage de civils seront peut-être épargnés. Grâce à l'intelligence artificielle, peut-être que les robots de demain éprouveront les mêmes sentiments que les humains : haine, jalousie, peur, qui peuvent d'ailleurs être à l'origine des conflits et des guerres. Nous sommes là face à des questions éminemment philosophiques.

Pour répondre à M. Larsonneur sur la vulnérabilité et la dépendance technologique : oui, cette dépendance est aujourd'hui majeure et nous devons être conscients que l'on retrouve chez nos rivaux comme chez nos alliés un écosystème qui produit une sorte de consanguinité entre l'armée et l'industrie numérique. Il s'agit d'un complexe « militaro-numérique ». Tel est le cas en Chine avec les BATX – pour Baidu, Alibaba, Tencent et Xcaomi – ou aux États-Unis avec les GAFA, auxquels on ajoute parfois un M pour Microsoft. La plupart des applications que nous retrouvons sur nos appareils numériques sont aujourd'hui issues de la recherche militaire et ces technologies sont par la suite transférées à l'industrie numérique. Celle-ci les développe et en fait des outils formidables grâce auxquels nous achetons nous-mêmes des millions de produits, qui génèrent des milliards d'euros de profit, qui sont ensuite réinvestis dans la recherche à vocation militaire. Nous l'avons par exemple constaté chez Amazon, qui gère le *cloud computing* pour la CIA et le Pentagone.

Il faut donc qu'au niveau national – ou européen, si l'on considère que la souveraineté doit s'exprimer à ce niveau – nous nous donnions les capacités et les moyens d'avoir nous aussi nos champions numériques. Il en va non seulement de notre capacité à continuer à combattre et à nous défendre – y compris face aux menaces hybrides –, mais également de notre souveraineté et du succès des armes de la France. À travers le numérique, nous ne faisons pas uniquement face à des enjeux de souveraineté militaire, nous sommes face à des choix philosophiques dont dépend pour partie l'avenir de notre humanité.

M. le président. Je remercie les rapporteurs pour toutes ces précisions. Le compte rendu de cette réunion figurera dans le rapport. Si les rapporteurs souhaitent apporter des éléments complémentaires aux questions posées, celui-ci pourra être complété.

Mes chers collègues, dès lors que tout le monde s'est félicité de la qualité de ce rapport, je vous propose de le rendre public !

*La commission **autorise** à l'unanimité le dépôt du rapport d'information sur les enjeux de la numérisation des armées en vue de sa publication.*

ANNEXES

ANNEXE 1 :

AUDITIONS DE LA MISSION D'INFORMATION

(Par ordre chronologique)

➢ **État-major des armées – M. le général de division aérienne Bruno Maurice**, officier général chargé de la transformation digitale des armées ;

➢ **Grand équipement national de calcul intensif (GENCI) – M. Philippe Lavocat**, président-directeur général, **Mme Marie-Hélène Vouette**, responsable de partenariats, conseillère chargée des relations institutionnelles, et **M. Stéphane Requena**, directeur de la technique et de l'innovation ;

➢ **Institut national de recherche en informatique et en automatique (INRIA) – M. Antoine Petit**, président-directeur général, et **Mme Isabelle Ryl**, directrice du centre de Paris ;

➢ **Gendarmerie nationale – M. le colonel Eric Freyssinet**, chef de la mission numérique de la direction générale de la gendarmerie nationale ;

➢ **Table ronde académique :**

– **M. Gérard de Boisboissel**, ingénieur au centre de recherche des écoles de Saint-Cyr à Coëtquidan (CREC), secrétaire général de la chaire de cyberdéfense et de cybersécurité des écoles de Saint-Cyr ;

– **Mme Frederick Douzet**, professeur à l'université Paris-VIII, titulaire de la chaire Castex de cyberstratégie de l'Institut des hautes études de la Défense nationale (IHEDN) ;

– **M. Patrick Hebrard**, responsable de l'innovation et de la recherche en cybernétique de Naval Group, ancien titulaire de la chaire de cyberdéfense des systèmes navals de l'École navale ;

– **M. Yvon Kermarrec**, professeur à l'École nationale supérieure Mines–Télécom Atlantique et représentant de la chaire de cyberdéfense des systèmes navals de l'École navale ;

– **M. Fabien Lacoste**, responsable de la cybersécurité et l'intelligence artificielle à la direction de l'innovation de Naval Group ;

– **M. Axel Legay**, directeur de la chaire de cybersécurité sur l'analyse de la menace de l'INRIA ;

– **M. Paul Théron**, co-titulaire de la chaire de cyber-résilience aérospatiale » de l'École de l'air à Salon-de-Provence.

➢ **Table ronde industrielle :**

– **Groupement des industries françaises aéronautiques et spatiales (GIFAS) – M. Éric Trappier**, président, **M. le général (2s) Pierre Bourlot**, délégué général, **MM. Jérôme Jean**, directeur des affaires publiques, **Guillaume Muesser**, directeur des affaires économiques et de défense, et **Bruno Giorgianni**, directeur de cabinet du président ;

– **Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT) – M. Stéphane Mayer**, président, **M. le général (2S) Jean-Marc Duquesne**, délégué général, et **M. François Mattens**, directeur de la communication et des affaires publiques ;

– Groupement des industries de construction et activités navales (GICAN) – MM. François Lambert, délégué général, **Hervé Croce**, responsable des relations institutionnelles et des affaires de défense, **Éric Papin**, directeur de l'innovation et de la maîtrise technique de Naval Group, et **Mme Marie-Colombe Celerier**, responsable des relations extérieures de Naval Group.

➢ **Direction générale de l'armement – Mme l'ingénieur général de l'armement Caroline Laurent**, directrice de la stratégie, et **M. Jérôme Lemaire**, chargé de mission sur la numérisation des systèmes opérationnels et l'intelligence artificielle ;

➢ **Comité Richelieu – MM. Thierry Gaiffe**, président de la commission de la défense, **Nicolas Corouge**, vice-président, et **Jean Delalandre**, délégué général ;

➢ **État-major de l'armée de terre – M. le général Bernard Barrera**, sous-chef d'état-major chargé des plans et des programmes, **M. le colonel Olivier Kempf**, chargé de mission sur la cyberdéfense et la digitalisation, **M. le colonel Éric Estrella**, chef du bureau des systèmes d'information et de communication, **M. le colonel Claude Chary**, responsable de la simulation et de la recherche opérationnelle, et **M. le lieutenant-colonel Pierre Desquesses**, officier chargé des relations parlementaires ;

➢ **Agence nationale de sécurité des systèmes d'information (ANSSI)** – **M. Guillaume Poupard**, directeur général ;

➢ **M. le capitaine Jean-Baptiste Colas**, officier de programme Auxylium et conseiller chargé de l'innovation à la direction générale de l'armement ;

➢ **Direction générale des systèmes d'information de communication (DGSIC) du ministère des Armées – M. l'amiral Arnaud Coustillière**, directeur général, **M. Georges Soleil**, sous-directeur de la stratégie, et **M. Charles Verdier**, chef du bureau de la politique des systèmes d'information de communication ;

➢ **Secrétariat général pour l'administration du ministère des Armées – MM. Paul Serre**, directeur, adjoint au secrétaire général, et **Olivier Simon**, délégué aux systèmes d'information d'administration et de gestion ;

➢ **Thales – M. Marc Darmon**, directeur général adjoint du groupe et directeur général de l'activité relative aux systèmes d'information et de communication sécurisés, et **Mme Isabelle Caputo**, directrice des relations parlementaires et politiques ;

➢ **M. Josepth Henrotin**, rédacteur en chef de la revue DSI, chargé de recherches au Centre d'analyse et de prévision des risques internationaux (CAPRI) et à l'Institut de stratégie et des conflits (ISC) ;

➢ **Direction du renseignement militaire – M. le général Jean-François Ferlet**, directeur ;

➢ **État-major de l'armée de l'air – Mme la commissaire générale Françoise Latour**, chargée de mission auprès du major-général de l'armée de l'air, **M. le colonel Etienne Faury**, chef du bureau des plans à l'état-major de l'armée de l'air et **M. lieutenant-colonel Frédéric Ledoux**, officier correspondant d'état-major chargé du commandement et de la maîtrise de l'information ;

➢ **État-major de la marine nationale – M. l'amiral François Moreau**, sous-chef d'état-major chargé des plans et des programmes, **M. le capitaine de vaisseau Laurent Célérier**, *chief data officer* de la marine nationale et **M. le capitaine de vaisseau Dominique Caillé**, officier chargé des liaisons parlementaires ;

➢ **Direction générale de la sécurité extérieure (DGSE) – MM. Patrick Pailloux**, directeur technique, et **Philippe Ullmann**, conseiller chargé de la communication et des relations avec le Parlement ;

➢ **Facebook – M. Anton Maria Battesti**, responsable des affaires publiques pour la France, et **Mme Ophélie Gerullis**, responsable des politiques publiques pour la France.

ANNEXE 2 :

DÉPLACEMENTS DES RAPPORTEURS

(Par ordre chronologique)

1. <u>DGA Lab (16 janvier 2018)</u>

➢ **l'équipe d'animation du DGA Lab**, coordonnée par **M. Axel Dyèvre** ;

➢ les dirigeants de quatre *start-up* engagées dans les travaux du DGA Lab : **UserCube**, **Virdys**, **Gladys** et **Golden Bees**, ainsi que leurs correspondants au sein du ministère des Armées ;

2. <u>12e régiment de cuirassiers à Olivet (18 janvier 2018)</u>

➢ **M. le lieutenant-colonel Christophe de Reviers de Mauny**, commandant le 12e régiment de cuirassiers par suppléance ;

➢ les officiers, sous-officiers et militaires du rang chargés de la conduite des « projets éclaireurs » de l'armée de terre en matière de numérisation des procédures ;

➢ les officiers, sous-officiers et militaires du rang des escadrons de chars du régiment ;

3. <u>Site de Naval Group à Ollioules (30 janvier 2018)</u>

➢ **M. Éric Papin**, directeur de l'innovation et de la maîtrise technique de Naval Group ;

➢ **M. Julien Mifsud**, directeur du site ;

➢ **M. Cyril Lévy**, directeur des systèmes de drones de Naval Group ;

➢ **M. Philippe Méléard**, directeur de l'architecture des « systèmes de systèmes » de Naval Group ;

➢ **M. Christophe Bexas**, architecte des systèmes d'information des programmes Barracuda et SNLE 3G ;

➢ **M. Patrick Radja**, autorité technique pour la cybersécurité ;

➢ les personnels de Naval Group chargés de la plateforme d'intégration, de validation et de certification du système de direction de combat (***Combat Management System*, CMS**) des frégates multi-missions, du projet de « centre opérationnel du futur » des navires de surface, et du centre opérationnel de soutien intégré numérique ;

4. <u>Washington, États-Unis (du 11 au 15 février 2018)</u>

➢ **S.E. M. Gérard Araud**, ambassadeur de France ;

➢ à la **Chambre des Représentants** des États-Unis : **M. Ro Khanna**, représentant de la Californie, et les responsables du secrétariat de la commission de la Défense ;

➢ **M. l'ingénieur en chef de l'armement Nicolas Tessaud**, attaché d'armement, et **M. l'ingénieur en chef de l'armement William Fuller**, attaché d'armement adjoint ;

➢ **Mme Laure Pallez**, conseillère économique adjointe ;

➢ au ***Department of Defense*** : **Mme Essye Miller**, *Chief Information Officer* par intérim, et ses adjoints :

– **M. Brian Teeple**, adjoint en charge des fonctions dites de « C4&IIC », pour *Command, Control, Communications & Computers* (C4) – pour : commandement et conduite, transmissions et ordinateurs – et *Information Infrastructure Capabilities* (IIC) – pour : capacités d'infrastructures informatiques ;

– **M. Edward Brindley**, adjoint en charge de la cybersécurité ;

– **M. Randall Conway**, adjoint à la CIO en charge de la gestion de l'information du ministère (*Information Enterprise*) ;

➢ à la ***Defense Advanced Research Projects Agency*** (DARPA) – Agence des projets de recherche avancée de la Défense : **M. Brian Pierce**, directeur du service de l'innovation dans l'information (*Information Innovation Office*) ;

➢ au ***Strategic Capabilites Office*** (SCO) du *Department of Defense* : M. William Roper, directeur ;

➢ à l'état-major du **corps des *Marines*** : **M. le colonel Howard Marotto**, directeur adjoint du service de la logistique de nouvelle génération en charge de l'innovation et de la fabrication additive ;

➢ à la ***Dwight D. Eisenhower School for National Security and Resource Strategy*** : **M. le colonel Paul Gillespie** et **M. Steeve Bloor**, professeurs ;

➢ au ***Center for Cognitive Government*** **d'IBM** : MM. Joseph Cubba, vice-président chargé de la défense et du renseignement, Steve Stewart, directeur des affaires publiques et de la règlementation, Michael DiPaula-Coyle, son adjoint, et Mme Jennifer Ciarrocca, responsable du *Center for Cognitive Government* ;

➢ chez ***Amazon Web Services***, **Mmes Maria Saab, Erica McCann et Iram Ali**, responsables des affaires publiques ;

➢ à la ***Software & Information Industry Association*** (SIIA) – syndicat des industries des technologies de logiciels et de l'information : **M. Carl Schonander**, directeur des affaires internationales ;

5. 1er régiment d'hélicoptères de combat à Phalsbourg (29 mai 2018) :

➢ **M. le lieutenant-colonel Pierre Letzelter**, commandant le 1er régiment d'hélicoptères de combat par suppléance ;

➢ les officiers, sous-officiers et militaires du rang des escadrilles du régiment.