ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mercredi
30 mai 2018
Séance de 9 heures 30

Compte rendu n° 65

SESSION ORDINAIRE DE **2017-2018**

Présidence de M. Jean-Jacques Bridey, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures trente.

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.*

La séance est levée à onze heures cinquante-cinq.

*

* *

Membres présents ou excusés

Présents. - M. Damien Abad, M. François André, M. Pieyre-Alexandre Anglade, M. Jean-Philippe Ardouin, M. Florian Bachelier, M. Xavier Batut, M. Thibault Bazin, M. Olivier Becht, M. Christophe Blanchet, Mme Aude Bono-Vandorme, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. Philippe Chalumeau, M. André Chassaigne, M. Alexis Corbière, M. Jean-Pierre Cubertafon, M. Stéphane Demilly, Mme Marianne

Dubois, M. M'jid El Guerrab, M. Olivier Faure, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, Mme Pascale Fontenel-Personne, M. Claude de Ganay, M. Thomas Gassilloud, Mme Séverine Gipson, M. Guillaume Gouffier-Cha, Mme Émilie Guerel, M. Jean-Michel Jacques, Mme Élodie Jacquier-Laforge, Mme Manuéla Kéclard-Mondésir, M. Loïc Kervran, Mme Anissa Khedher, M. Bastien Lachaud, M. Fabien Lainé, Mme Frédérique Lardet, M. Jean-Charles Larsonneur, M. Christophe Lejeune, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, M. Joaquim Pueyo, M. Gwendal Rouillard, M. Pacôme Rupin, M. Thierry Solère, Mme Sabine Thillaye, Mme Laurence Trastour-Isnart, Mme Nicole Trisse, M. Charles de la Verpillière

Excusés. - M. Luc Carvounas, M. Laurent Furst, M. Christian Jacob, M. Jean-Christophe Lagarde, M. Franck Marlin, M. François de Rugy, M. Antoine Savignat