ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition conjointe, ouverte à la presse, de M. le contrôleur général des armées Christophe Jacquot, chef du service de la transformation, de M. le colonel Pierre-Yves Caniotti, chef de la division stratégie, prospective et partenariats du ComCyberGend, du général de brigade Patrick Perrot, chargé de mission au service de la transformation, sur la culture numérique et scientifique de la gendarmerie et sa préparation aux enjeux de demain.

Mercredi 2 février 2022
Séance de 9 heures

Compte rendu n° 41

SESSION ORDINAIRE DE **2021-2022**

Présidence de Mme Françoise Dumas, *présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

Mme la présidente Françoise Dumas. Ancrée dans l'ADN du gendarme, la capacité d'innovation est un vecteur majeur du processus de transformation de la Gendarmerie nationale. Cette mission est assurée par le département de la prospective et de l'innovation du service de la transformation, qui fournit aux gendarmes les matériels et équipements les plus adaptés à leurs besoins. Il serait intéressant que vous nous indiquiez comment votre service encourage les initiatives innovantes, comment vous captez les innovations en provenance de la base et comment vous faites remonter du terrain les bonnes initiatives locales. Par ailleurs, qu'attendez-vous de l'intelligence artificielle (IA) ?

Le directeur général de la gendarmerie nationale, le général Christian Rodriguez, nous indiquait qu'en 2021, 52 % des officiers recrutés étaient des ingénieurs ou des titulaires d'un master 2 en sciences dures. En quoi ce modèle de recrutement constitue-t-il un atout pour votre force armée ?

Comme le directeur général nous l'expliquait la semaine dernière, le cyberespace est désormais massivement investi par la criminalité sous toutes ses formes, ce qu'il qualifie de nouvelle frontière de la délinquance. C'est pourquoi, en février 2021, a été créé par arrêté le Commandement de la gendarmerie dans le cyberespace, ou ComCyberGend, directement rattaché à la direction générale de la gendarmerie nationale (DGGN) et localisé sur le cybercampus de la Défense. L'objectif de ce nouveau commandement est de regrouper l'ensemble des forces cyber de la gendarmerie afin de les faire gagner en cohésion et en cohérence et de créer une vraie filière cyber. Il serait intéressant que vous décriviez l'organisation et l'activité du ComCyberGend depuis sa création et que vous évoquiez comment votre réseau de cyber-patrouilleurs et d'enquêteurs numériques est structuré. Le général Rodriguez mentionnait les e-compagnies ou compagnies numériques. De quoi s'agit-il ? Nous souhaitons également savoir comment vous réussissez à recruter les compétences rares dans ces domaines et comment vous sensibilisez l'ensemble des gendarmes aux enjeux de la cybersécurité. Le général Rodriguez évoquait la souplesse dont il bénéficiait pour recruter des « geeks » et la création possible d'une école du cyber dont, je l'espère, vous pourrez nous parler un peu plus. Parvenez-vous à fidéliser ces « geeks » ou se font-ils rapidement débaucher par le secteur privé ?

Enfin, notre commission, dont plusieurs membres sont d'ailleurs réservistes, est très attachée à nos réserves militaires. Il serait intéressant que vous nous expliquiez comment les réservistes sont mobilisés dans votre arsenal de cybersécurité.

M. le contrôleur général des armées Christophe Jacquot, chef du service de la transformation. Je suis chef du service de la transformation, depuis sa création en 2020. Je propose de vous apporter un éclairage sur la transformation en gendarmerie et sur l'innovation, qui en est un levier fondamental, en lien étroit avec les ministères des Armées.

La transformation s'entend comme l'adaptation dynamique et continue aux évolutions de son environnement, des nouveaux usages, des attentes de la population et des élus, des évolutions sociétales, juridiques et technologiques. Pour répondre à l'ensemble de ces bouleversements et tenir compte de leur accélération, le service a pour mission de piloter l'exécution du plan stratégique du directeur général – plan GEND 20.24 – qui place la

population au cœur de la mission et fait du gendarme son principal exécutant. Ce plan s'articule autour de quatre orientations fondamentales regroupant 84 projets de transformation lancés depuis janvier 2020.

Le premier pilier consiste à mieux protéger en développant une offre sur-mesure. Je pense en particulier à l'amélioration de la réponse opérationnelle qui vous a déjà été présentée par le dispositif de gestion des événements (DGE) ainsi qu'au principe de redevabilité et au dispositif de consultation et d'amélioration du service (DCAS), qui pose les bases d'une véritable co-construction de la sécurité avec les élus. Je pense également à la brigade numérique et au ComCyberGend, que le colonel Caniotti décrira tout à l'heure.

Le deuxième pilier consiste à mieux progresser en s'engageant ensemble et en confiance. Plusieurs outils ont été mis en place à cette fin. Il s'agit par exemple des *chatbots* de ressources humaines qui permettent à tout un chacun de visualiser son parcours au sein de la gendarmerie ou des différents *massive open online courses* (MOOC) organisés, en particulier celui consacré à l'IA qui sera évoqué par le général Perrot.

Le troisième pilier consiste à mieux équiper en construisant le futur dès à présent. J'évoquerai à ce titre le pack mobilité, qui favorise l'exercice des missions du gendarme au plus près de la population et qui se compose d'un ordinateur *Ubiquity*, disposant de capacités de consultation et de traitement identiques à celles d'un ordinateur dans une brigade, ainsi que d'un smartphone deuxième génération, le NEO 2, associé à 74 applications. Il s'agit encore du projet GendFabLab, qui permet l'impression en 3D au sein de chaque groupement et qui a émergé en particulier pendant la première crise du covid.

Le dernier pilier consiste à mieux fonctionner en allégeant la contrainte et en libérant les solutions. Nous pouvons citer le projet P4S, assistant à l'élaboration du service qui facilite grandement le travail du commandant de brigade, ainsi que le vote par voie électronique que nous avons favorisé pour le travail de concertation du Conseil de la fonction militaire de la gendarmerie.

En résumé, nous avons pour missions d'anticiper les évolutions, d'accompagner les projets de transformation et de les valoriser, afin de donner au directeur général une vision à la fois globale, actuelle et transverse de l'ensemble des projets de transformation tout en facilitant l'émergence de nouveau projets et l'adoption de nouveaux modes de travail, davantage transversaux, collaboratifs et créatifs.

J'en viens ainsi au sujet de l'innovation en gendarmerie, qui est en réalité le reflet d'un savant dosage d'audace, de créativité et d'adaptation au terrain. En effet, ce que l'on attend d'une innovation, c'est qu'elle facilite l'exercice de la mission du gendarme au service de la population. Un plan de stratégie de recherche et d'innovation a ainsi été mis en place, prolongeant en quelque sorte le plan stratégique GEND 20.24 du directeur général. Celui-ci structure véritablement notre ambition sur le long terme, avec des objectifs clairement définis : faire du cyberespace une priorité, s'engager dans une stratégie d'ouverture de la donnée, mettre en place une IA de confiance au service de la sécurité, placer l'humain au cœur de la transformation numérique, développer la recherche et l'innovation dans les sciences du vivant, au profit des enquêtes judiciaires comme d'une biométrie raisonnée et enfin durcir la protection, alléger l'équipement et augmenter les capacités du gendarme.

Je souhaiterais développer ce dernier point, qui tire les conséquences de l'évolution du contexte d'intervention du gendarme, à savoir une violence d'intensité croissante dans l'environnement des élus comme dans l'environnement intrafamilial ou dans celui de la délinquance. C'est pourquoi il nous faut nous montrer vigilants sur les fondamentaux de l'identité militaire et les aptitudes du commandement à remplir nos fonctions et notre contrat opérationnel. C'est une véritable éthique de l'action qui gouverne l'activité des gendarmes, constituée des vertus et des valeurs associées et héritées de notre appartenance à la collectivité militaire, qui doivent sans cesse être cultivées. Pour accroître cette protection du gendarme, je citerai l'exemple du pack équipement individuel ou du gilet d'intervention trois en un, sorte de gilet pare-balles transformable.

Pour mettre en œuvre cette stratégie de recherche et d'innovation, la gendarmerie peut compter sur un écosystème qui assure le continuum entre l'innovation ouverte, l'innovation dirigée et l'innovation participative, jusqu'au développement industriel. La gendarmerie s'appuie sur l'innovation ouverte, notamment vers les mondes académique et industriel, afin de détecter les technologies dites « de rupture », qui sont en réalité les technologies de demain, pour répondre le mieux possible aux défis à venir. La gendarmerie constitue aujourd'hui une communauté de 300 docteurs et doctorants animée par le Centre de recherches de l'école des officiers de la gendarmerie nationale (CREOGN) et s'inscrit véritablement dans une logique partenariale de recherche fondamentale à finalité opérationnelle, sur la base de 150 accords de collaboration : des accords-cadres avec des partenaires académiques publics, comme avec le Centre national de la recherche scientifique (CNRS), et des accords avec l'Institut national de recherche en sciences et technologies du numérique (INRIA), avec l'Agence de l'innovation défense (AID) partenaire essentiel, ainsi qu'avec l'Office national d'études et de recherches aérospatiales (ONERA).

La gendarmerie s'engage également dans un dialogue avec le secteur privé de l'industrie de défense et de sécurité en particulier, notamment à travers le Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT). C'est dans ce cadre qu'elle a organisé, en décembre dernier, l'accompagnement par la gendarmerie de l'innovation, de l'industrie et de la recherche (AGIIR), à la Station F, salon qui s'est concrétisé par des rencontres entre des industriels, notamment des jeunes pousses, et des directeurs de programmes et des chefs de projet de la DGGN.

Pour développer cette culture scientifique et de l'innovation, il est apparu indispensable d'accroître notre ressource scientifique. C'est ainsi qu'en 2021, 52 % des officiers recrutés étaient des ingénieurs ou des personnes titulaires d'un master à dominante scientifique.

Je ne ferai que citer l'innovation dirigée, qui ressort d'une démarche capacitaire, pour consacrer la fin de mon propos à l'innovation participative, à l'accompagnement et à la valorisation des innovations. La démarche participative est un fleuron de la gendarmerie dans la mesure où elle crée une véritable dynamique collective. Elle repose sur une idée simple – celui qui sait est celui qui fait, et sur un principe clairement énoncé par notre directeur général : le droit à l'erreur. Par le biais d'une *hotline*, grâce à laquelle tout personnel de la gendarmerie peut poser une question à la DGGN, mais surtout grâce à un dispositif d'ateliers d'innovation, rénové en 2021, l'échelon central recueille, sans filtre hiérarchique, les propositions et innovations mises en œuvre au plan local. Celles-ci sont proposées à un comité de suivi de la DGGN, qui a pour mission d'élaborer uniquement avis d'innocuité.

Autrement dit, l'administration centrale doit émettre un véritable avis pour s'opposer à une innovation. L'innovation est ensuite ouverte à un vote des utilisateurs. Tout personnel de la gendarmerie peut ainsi s'exprimer sur les meilleures innovations selon le principe suivant : le terrain juge le terrain. Puis les innovateurs voient leur innovation publiée, voire généralisée à l'ensemble de la gendarmerie, les meilleurs étant récompensés lors d'une cérémonie qui leur est consacrée. C'est ainsi que le département de la prospective et de l'innovation (DPI) de mon service anime une véritable communauté d'innovateurs et également de *makers,* terme aujourd'hui consacré aux créateurs d'objets dans le milieu de l'impression 3D au service de la sécurité. En quinze ans, environ 1 880 bonnes pratiques ont été présentées, dont 780 ont été retenues et environ 10 % généralisées ou proposées à une réplication ou à un partage. Je citerai deux exemples récents : la borne pass sanitaire (qui vérifie la validité d'un pass en flashant un QR code), mis à disposition sur internet en licence ouverte, ainsi que l'application Gendluxe, disponible sur NEO, qui permet aux gendarmes de constater plus efficacement, plus facilement et plus rapidement les infractions liées à la contrefaçon de produits de luxe. En complément de ce dispositif et pour stimuler l'innovation au sein d'un service particulier, il arrive également que nous organisions des hackathons, comme celui qui se tiendra en avril prochain sur le thème du *speech to text*, c'est-à-dire la transcription du langage oral en langage écrit, avec une école d'ingénieurs partenaire, des ateliers d'idéation, des défis participatifs pour des sujets très concrets (fabrication des visières pendant la crise covid, aménagement sécurisé de coffres de véhicules, etc.). De nombreux projets sont en cours, dont certains sont communs aux Armées et à la gendarmerie, et sont naturellement soutenus par l'AID, tels que NEODK, dispositif mobile de relevé d'empreintes décadactylaires qui évite le déplacement à la brigade et permet d'envoyer au fichier les éléments retenus.

En matière d'accompagnement de la valorisation, le service de la transformation anime à échéance mensuelle une commission de valorisation des innovations qui associe la direction des opérations de l'emploi (DOE) mais aussi la direction des soutiens et des finances (DSF). L'objectif est d'accompagner les innovations dès le départ en fonction de leur degré de maturité, c'est-à-dire de leur donner des conseils de nature juridique, technique, financière, mais aussi de choisir le moyen le plus efficace pour orienter une innovation. Avons-nous atteint le stade de partenariat industriel ? Souhaitons-nous intégrer cela à une démarche capacitaire ou souhaitons-nous déposer un brevet ? Récemment, le drone *indoor* de criminalistique HANGI a été primé par la ministre des Armées. Celui-ci, au lieu de posséder une hélice extérieure, fonctionne sans troubler l'environnement par le brassement de l'air et peut également être utilisé pour la sécurité d'événements particuliers dans des halls fermés. Nous pouvons aussi citer l'exemple de SGATI, balise de *tracking* basse consommation reposant non pas sur une technologie GPS classique mais sur la technologie *Internet of Things* (IoT). C'est ainsi que la gendarmerie a déposé dix brevets, dont celui pour une colle conductrice électrique, celui pour un dispositif de prélèvement de matière osseuse, en lien avec le Muséum national d'histoire naturelle, fortement intéressé par cette innovation, et enfin celui pour le laboratoire mobile d'analyse ADN.

En conclusion, l'innovation est inhérente à l'identité du gendarme. C'est un écosystème qui repose sur l'humain et sur la prise en compte du terrain, pour faire se rencontrer des besoins et des idées, et c'est en s'appuyant sur nos fondamentaux militaires et sur un plan stratégique que l'institution peut anticiper les défis et les attentes des citoyens et des élus en matière de sécurité comme de protection.

M. le général Patrick Perrot, chargé de mission au service de la transformation. J'interviendrai sur un sujet à la fois très spécifique et fondamental, celui de l'IA, notamment dans le domaine de l'innovation. « Le futur dès à présent », plus qu'un slogan, est un objectif affirmé dans le cadre du plan stratégique voulu par notre directeur général. Il s'agit donc bien de préparer l'institution aux enjeux de demain, avec pour objectif de mieux protéger la population, tant sur le plan individuel que sur le plan collectif. Nous pensons que l'IA est particulièrement adaptée à cette ambition grâce à ses capacités d'adaptation et d'anticipation.

Quels sont les enjeux de demain ? Le premier est un enjeu de souveraineté. Il faut dès aujourd'hui se poser la question de la gouvernance des nouveaux territoires numériques, c'est-à-dire des territoires connectés, des mondes réels ainsi que des métavers, ou mondes virtuels, mus par l'IA. La question de la souveraineté en matière de sécurité de ces différents espaces est primordiale, dans la mesure où l'on constate une mainmise des géants du numériques – GAFA et BATX – sur ceux-ci. Quelle place la gendarmerie nationale occupe-t-elle au sein de ces territoires ?

Le deuxième enjeu est celui de la protection de la population. Comment faire face, aujourd'hui, à une délinquance de plus en plus déhiérarchisée, mais surtout de plus en plus équipée technologiquement ? Cette dernière possède actuellement les moyens d'agir à moindre risque mais à coût maximum. Ces observations concernent la criminalité organisée, le terrorisme, mais aussi la délinquance de droit commun, grâce aux outils désormais à sa portée.

Le troisième enjeu est celui du service à l'usager. Comment la gendarmerie peut-elle aujourd'hui apporter un service égal à l'ensemble de nos concitoyens, où qu'ils se trouvent sur le territoire ? Cela pose la question de l'accessibilité au service, de la redevabilité vis-à-vis du citoyen ainsi que de l'égalité du service rendu.

Pour faire face à ces enjeux, nous avons choisi de considérer l'IA non pas comme une discipline informatique – ce qu'elle n'est d'ailleurs pas – mais comme un vecteur de transformation de notre offre de protection de la population et de nos processus métiers. Nous avons adopté à cet effet une stratégie plurielle « à 360 degrés » reposant sur un certain nombre de piliers.

Le premier d'entre eux est celui de la formation, dans la mesure où il n'existe pas d'IA sans connaissances. C'est à ce titre que notre institution recrute aujourd'hui de nombreux scientifiques. La formation permet d'éviter tout effet de boîte noire et de mieux appréhender l'IA comme une aide à la décision. Il s'agit de former nos cadres de demain à décider avec l'apport de l'IA et surtout, à savoir ne pas abandonner leur pouvoir de décision. En effet, le problème ne vient pas de la machine, mais plutôt de l'humain, qui pourrait abandonner ce pouvoir décisionnel comme nous le faisons quotidiennement, pour prendre un exemple concret, lorsque nous utilisons notre GPS. Cette situation est anodine et ne porte pas à conséquence, ce qui n'est pas le cas des prises de décisions opérationnelles, tactiques ou stratégiques, où les effets peuvent s'avérer bien plus graves. La formation assure en outre l'aspect non-discriminatoire de l'IA, qui est quant à elle par définition discriminante. Notre formation s'échelonne à trois niveaux. Il s'agit tout d'abord de l'acculturation. 87 % de nos gendarmes, soit un chiffre considérable, ont suivi le MOOC « Objectif IA » d'OpenClassrooms. Pour compléter ce MOOC, qui se veut généraliste, nous produisons, à un rythme bimestriel, une revue d'une dizaine de pages intitulée Culture IA, ayant pour vocation

de poser les bases de l'IA dans le domaine de la sécurité intérieure (questions de reconnaissance spatiale, de reconnaissance du locuteur, d'analyses prédictives, etc.), mais aussi d'informer de façon plus générique sur l'IA. Le deuxième étage est celui de la sensibilisation à l'information. Dès la formation initiale, nous construisons une offre, d'une durée de deux à quatre heures, pour sensibiliser nos gendarmes à l'IA et tout au long de leur carrière, des points de rappel sont proposés selon des cadences régulières. Le troisième étage est celui de la formation à proprement parler, à deux niveaux. Les officiers, à mi-carrière, ont la possibilité d'effectuer une scolarité alternative et de se spécialiser en IA. Récemment, nous avons créé, avec l'Institut supérieur d'électronique de Paris (ISEP), une chaire « IA et Sécurité ». Nous proposons ainsi des parcours doctoraux à certains de nos officiers.

Le deuxième pilier est celui de la recherche, puisqu'il convient d'avoir un temps d'avance sur l'adversaire afin de pouvoir faire face à une délinquance de plus en plus technologique. Nous collaborons avec des centres de recherche, par exemple le Centre d'études des radicalisations et de leurs traitements (CERT) de l'Université de Paris, avec *l'Artificial and Natural Intelligence Toulouse Institute* (ANITI) et avec l'Institut interdisciplinaire de 3IA Côte d'Azur, sur la chaire *smart city* et philosophie. Nous publions certains de nos travaux dans des revues scientifiques mais également dans des revues destinées à l'ensemble des citoyens afin de leur expliquer ce que nous faisons, dans un souci de transparence. Nous participons par ailleurs à des projets européens et depuis peu, nous avons accès au supercalculateur Jean Zay.

Le troisième pilier est celui du développement, qui doit prévenir l'effet boîte noire : nous devons maîtriser les outils que nous allons utiliser. Cela ne signifie pas que nous ne choisissons pas de solutions commerciales mais, le cas échéant, nous saurons comment celles-ci fonctionnent. Le développement que nous avons conduit jusqu'ici se situe dans le domaine de l'analyse prédictive de la délinquance à des fins de prévention, qui nous apporte plus de transparence vis-à-vis des autorités administratives et judiciaires, des élus ainsi que des citoyens. Nous travaillons par ailleurs à l'analyse des relations entre entités au sein des réseaux criminels de façon à mieux contrôler le rôle de chacun. Nous travaillons sur les problématiques de discrimination dans le domaine de la reconnaissance faciale. Nous travaillons encore sur l'authentification des *deepfakes*, hypertrucages très à la mode qui reposent sur des réseaux génératifs adverses et qui envahissent notre quotidien. Nous travaillons à la synthèse automatique de textes ainsi qu'au vieillissement et au rajeunissement des individus dans le domaine de la police judiciaire. Nous avons également fait l'acquisition d'un *chatbot* dédié aux ressources humaines et nous en concevons de nouveaux.

Le quatrième pilier est celui de l'éthique et de la régulation. L'usage éthique de l'AI dans le domaine de la sécurité intérieure représente selon moi une condition primaire. Nous en avons regroupé les éléments essentiels au sein d'une charte : confiance, responsabilité, loyauté, respect et transparence. Cela nécessite également d'évaluer nos systèmes à partir du cadre éthique élaboré. Nous participons à des projets européens sur l'éthique des algorithmes ainsi qu'au projet de réglementation européen de l'IA.

Le cinquième pilier est celui des partenariats. L'IA demande à être challengée et comparée entre experts. Nous disposons de conventions avec le CNRS, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), le Conservatoire national des arts et métiers (CNAM) et la Conférence des grandes écoles (CGE). Par ailleurs, nous entretenons des liens étroits avec des *think tanks* tels que l'Institut EuropIA, avec Sophia Antipolis, qui

s'est fixé pour mission de rendre l'IA accessible à tous, avec le hub France IA, dans le domaine de l'IA et des ressources humaines ainsi que de l'IA et des territoires, avec l'Institut Sapiens, sur les enjeux éthiques, et avec l'AID, où deux de nos officiers sont actuellement affectés. Récemment, nous avons entrepris une collaboration avec l'éducation nationale afin d'expliquer nos actions en matière d'IA.

Le sixième pilier est celui de l'organisation et du management. L'IA doit ainsi non seulement servir à la population, mais aussi venir faciliter le travail du gendarme. Cela se traduit par l'utilisation du *chatbot*, que nous avons déjà évoqué, dans le but d'intégrer davantage d'humain dans le parcours de carrière de nos personnels, en libérant du temps pour nos gestionnaires de sorte qu'ils puissent s'engager plus profondément dans les entretiens et mieux examiner les dossiers. Par ailleurs, le *chatbot* répond à l'ensemble des questions qui peuvent être posées, vingt-quatre heures sur vingt-quatre, ce qui est cohérent avec les horaires décalés du gendarme. La gestion prévisionnelle des emplois et des carrières représente un autre aspect de management. L'IA doit ainsi permettre à chacun de s'approprier davantage son parcours, en termes de formation et d'évolution.

La vision stratégique que nous portons correspond à la vision européenne, puisque nous sommes co-présidents du groupe lié à la stratégie en matière d'IA au niveau européen.

Je conclurai par une phrase empruntée à Marie Curie : « Rien n'est à craindre, tout est à comprendre. » Il ne faut pas avoir peur de l'IA dans la mesure où cette discipline nous offre des opportunités considérables que nous devons saisir au lieu de céder l'avantage à l'adversaire, pour avancer et préparer les enjeux de demain.

M. le colonel Pierre-Yves Caniotti, chef de la division stratégie, prospective et partenariats du ComCyberGend. J'ai l'honneur de représenter le commandant de la gendarmerie dans le cyberespace, le général de division Marc Boget, qui ne pouvait être présent aujourd'hui. Je me propose de vous apporter un éclairage sur les missions de ce nouveau et grand commandement dans l'environnement complexe au sein duquel nous évoluons, qui nécessite une agilité particulière.

Le cyberespace n'est autre qu'un espace public dans lequel l'ensemble des missions de la gendarmerie trouve à s'appliquer, du renseignement à l'ordre public, et de la sécurité publique à la police judiciaire. La construction de la réponse à la menace cyber est donc particulièrement transverse, impliquant l'ensemble des échelons de commandement mais aussi des services spécialisés. Elle suppose par ailleurs des adaptations permanentes, l'année 2021 ayant été marquée par la création du ComCyberGend.

L'évolution des technologies et services numériques ainsi que l'adaptation continue des modes opératoires des organisations criminelles dresse un état de la menace qui donne le vertige. Sur le plan statistique, le constat est sans appel : l'impact est sérieux et en augmentation constante. Les faits rapportés à la gendarmerie sont en effet en hausse d'une année sur l'autre de 10 à 40 % selon les phénomènes criminels considérés. Le premier enjeu est donc de diminuer le nombre de victimes et d'accompagner celles que nous n'avons pu préserver. Le deuxième enjeu consiste à peser sur la délinquance en ayant à l'esprit que ces groupes criminels sont avant tout constitués en écosystèmes très dynamiques dans leur construction et leur infrastructure, le tout évoluant dans un environnement qui s'affranchit des frontières physiques. Le troisième enjeu est de garantir un haut niveau de compétence pour

composer avec l'évolution permanente des technologies et services numériques largement exploités par les organisations criminelles. Parmi les défis que nous relevons d'ores et déjà, figure celui de l'omniprésence numérique et du volume toujours plus important de données à traiter, qui oblige le gendarme à acquérir des compétences spécifiques en sus de l'ensemble des compétences métier qu'il détient déjà ; le défi du chiffrement, dont le développement nécessite la mise en œuvre de technologies de pointe et de modes d'action innovants ; le défi des cryptomonnaies, dont l'utilisation croissante suppose pour les enquêteurs de tracer ces actifs sur internet ; le défi du *cloud computing*, qui pose des questions juridiques prégnantes nécessitant la mise en place d'actions de coopération à l'international et de normes supranationales.

Pour répondre à ces enjeux, le directeur général a souhaité la création d'un grand commandement du cyber pour la gendarmerie. S'inscrivant pleinement dans sa stratégie GEND 20.24, il est opérationnel depuis le 1er août dernier. Sa vocation est de placer l'ensemble des unités exerçant une mission dans le cyberespace sous une bannière de coordination unique et parfaitement identifiable. Il incarne ainsi la composante numérique que toute mission de la gendarmerie comporte désormais. Il exerce ses missions sur l'ensemble du territoire en appui et au profit de l'ensemble des unités de la maison.

Le ComCyberGend assume d'abord dans le cyberespace l'un des impératifs majeurs de la gendarmerie au quotidien, la proximité numérique, autrement dit le lien avec la population qu'elle protège. En se rendant disponible sur l'espace public internet, en orientant l'usager et les victimes et en diffusant des messages de prévention en lien avec ses nombreux partenaires, il accompagne la transition et est doté à ces fins de structures de prévention, de contact et de première assistance en ligne. Fonctionnant vingt-quatre heures sur vingt-quatre et sept jours sur sept, magendarmerie.fr permet d'entrer en contact direct avec un gendarme. Nous avons pour cette unité un nombre de sollicitations en augmentation constante, de l'ordre de 300 à 600 par jour. Parallèlement, en partenariat avec l'ensemble des acteurs participant à diffuser une culture cyber auprès de la population, des acteurs économiques et des collectivités territoriales, le dispositif CyberGEND, pleinement intégré au maillage territorial de la gendarmerie, conduit des actions de prévention à l'aide de contenus élaborés au niveau central par le ComCyberGend et visant à une prise de conscience des dangers liés aux usages numériques afin de s'en prémunir et d'évoluer en sécurité sur les réseaux, participant ainsi à la confiance numérique.

Le ComCyberGend anime ensuite la fonction investigation sur le cyberespace, essentiel pour peser efficacement sur la cybercriminalité, mais aussi sur la criminalité usant du vecteur cyber pour augmenter sa surface d'attaque, pour diversifier ses activités ou les dissimuler. À cet effet, le ComCyberGend s'appuie une nouvelle fois sur le dispositif CyberGEND, qui constitue notre allonge dans les territoires et forme un réseau de 7 000 cybergendarmes aux compétences diverses – investigations simples sur support numérique, investigations complexes, recherches du renseignement sur internet, recherches en source ouverte, enquêtes sous pseudonyme ou encore traçabilité des cryptoactifs – permettant d'apporter en tout point du territoire une même qualité de traitement des faits cyber. Notre ambition est de porter ce dispositif à 10 000 cybergendarmes.

Le ComCyberGend s'appuie également sur le centre de lutte contre les criminalités numériques (C3N), qui lui est directement rattaché. Le C3N est l'unité de police judiciaire à compétence nationale de la gendarmerie en matière de lutte contre la cybercriminalité. Il se

décline en onze antennes régionales au sein des sections de recherche pour agir sur la cybercriminalité du haut du spectre, et nous souhaiterions les porter à trente dans le futur.

Enfin, le ComCyberGend repose sur des compétences techniques de haut niveau, partout sur le territoire, grâce à ses enquêteurs Ntech au sein des plateaux départementaux ainsi qu'à ses ingénieurs experts au niveau central en capacité de procéder à des actes d'investigation sur des supports numériques et d'être projetés sur le terrain lors de constatations, de perquisitions ou d'auditions dans des environnements complexes.

Face à l'événement, les principes militaires de subsidiarité des unités et de complémentarité des moyens président à notre action quotidienne. Suivant un impératif de réactivité, gage de notre efficacité opérationnelle, le dispositif intégré du ComCyberGend vient s'agréger aux échelons territoriaux de commandement et se combine naturellement, autant que de besoin, à d'autres compétences d'exception comme les négociateurs du groupe d'intervention de la gendarmerie nationale (GIGN) ou les spécialistes de certains milieux maritimes ou aéronautiques pour intervenir au plus vite et au plus près de chaque situation.

Que ce soit sur le segment de la prévention comme sur celui de l'investigation numérique, la gendarmerie s'inscrit résolument dans une démarche collaborative, avec l'ensemble des acteurs, parmi lesquels figurent, pour ce qui relève des actions de prévention plus particulièrement, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), cybermalveillance.gouv.fr ainsi que les associations d'élus et, pour ce qui relève de l'investigation, de nos collègues de la police nationale et des services de renseignement. Le ComCyberGend est également en relation permanente avec les partenaires étrangers, qu'il s'agisse des forces de sécurité intérieure étrangères partenaires comme des experts techniques nationaux de l'écosystème, au travers de groupes fermés d'experts permettant une interaction technique entre les acteurs. En outre, sur le segment de l'investigation, le ComCyberGend recherche systématiquement l'appui d'organismes supranationaux comme Europol afin de permettre à la gendarmerie d'agir efficacement en dehors de nos frontières. Par ailleurs, il contribue activement aux travaux préparatoires, législatifs et réglementaires au niveau national et normatifs au niveau supranational pour garantir aux forces de sécurité intérieure la capacité d'agir.

La militarité des gendarmes du dispositif CyberGEND s'exprime également par leur polyvalence. Se mêlent ainsi compétences métier, compétences techniques et compétences juridiques, que chaque acteur doit détenir, certes à des niveaux divers selon ses fonctions, mais suffisantes pour accompagner les victimes en tout point du territoire, quel que soit leur profil, et pour peser sur la délinquance. Une formation enrichie sur le volet numérique est dispensée aujourd'hui dès la formation initiale. Pour ceux qui témoignent d'emblée d'une appétence pour la matière cyber, des e-compagnies d'élèves gendarmes ont été créées afin de permettre à ces jeunes militaires d'acquérir des connaissances et des compétences dans le domaine de l'investigation numérique. Nous mettons également en œuvre une formation cyber pour tous qui s'appuie sur des formateurs relais dans chaque département et qui vise à diffuser largement une culture cyber dans nos rangs.

Pour nos enquêteurs spécialisés, nous avons développé – et continuons à développer – des partenariats avec des universités pour créer des formations mixtes permettant d'acquérir d'une part des compétences métier avec nos centres de formation, et d'autre part des compétences techniques à l'université. Ces formations sont qualifiantes puisqu'il s'agit de

licences professionnelles et de masters spécialisés labellisés par l'ANSSI. Enfin, une réflexion sur les compétences autour du cyber est conduite pour anticiper d'ores et déjà les évolutions à trois à cinq ans relatives aux métiers de l'investigation numérique, du traitement de la preuve numérique et aux métiers de la science de la donnée.

Nous réfléchissons également à la création d'un centre de formation cyber. La gendarmerie a fait des propositions en ce sens et des discussions sont en cours au ministère. Nous travaillons de longue date de concert avec la police nationale et le Centre européen de formation cyber (ECTEG) sur ces questions. Les lignes qui se dessinent à ce sujet sont une implantation en province, au sein d'un établissement qui serait à la fois le réceptacle d'un certain nombre de formations et le lieu où elles sont conçues, tout en ayant pour but de démultiplier les effets en décentralisant certaines formations sur le territoire, y compris en outre-mer. Ces formations auront également vocation à accueillir des partenaires, comme nous le faisons déjà parfois en recevant des fonctionnaires des douanes, des militaires du COMCYBER, des magistrats, etc.

Parallèlement, certains développements technologiques doivent être suivis de près : l'IA, le développement de la 5G, le développement des techniques de chiffrement et bien d'autres. L'appréhension de ces technologies de pointe et de leur impact sur la sécurité des citoyens nécessite le développement de compétences de haut niveau. La gendarmerie dispose à cette fin d'officiers docteurs et doctorants dans chacun de ces domaines. Certains militaires quittent la gendarmerie pour poursuivre leur parcours ailleurs, même si des passerelles leur sont proposées pour rejoindre d'autres institutions afin d'optimiser le temps de service au sein de l'État. Mais la majorité d'entre eux sont attachés à la mission de service public, à leur engagement et à la réalisation concrète de leurs investigations, des constatations à l'interpellation des mis en cause, jusqu'à soutenir leurs travaux au procès pénal. Vous ne trouverez nulle part ailleurs cette continuité d'action, particulièrement enrichissante et valorisante selon ma propre expérience.

Pour conclure, notre dispositif de lutte contre les cybermenaces place la victime au cœur de notre manœuvre, fonctionne selon un mode agile, veille à garantir une même qualité de traitement partout sur le territoire, par une approche intégrée et inclusive répondant à un proverbe que le général de division Marc Boget a fait sien : « Seul, on va plus vite. Ensemble, on va plus loin. » Ensemble, c'est aussi avec nos réservistes cyber. Selon notre dernier recensement, ils sont en nombre légèrement insuffisant et j'invite donc nos concitoyens à se signaler auprès de nos services pour nous rejoindre. La semaine dernière, nous avons réuni nos réservistes afin de leur présenter nos actions et de les associer à nos travaux portant sur la prévention, sur la conduite de projets, sur des missions d'appui opérationnel selon leurs profils et leurs appétences. Ces derniers sont pleinement mobilisés.

Mme Françoise Ballet-Blu. Vos présentations nous ont permis de saisir tous les enjeux de la prospective et des nombreuses transformations des menaces qui pèsent sur notre pays. En décembre 2020, la ministre des Armées Florence Parly a présenté le programme Red Team Defense, qui avait pour but de recruter des auteurs, des dessinateurs de bande dessinée et des scénaristes de science-fiction afin de composer un groupe de travail visant à imaginer des situations potentiellement dangereuses pour l'armée du futur. À la suite d'un appel à candidatures, plus de 1 200 CV ont été reçus et, si les critiques les plus virulentes émanaient du monde de la science-fiction lui-même, l'AID, à l'origine du projet, se félicite des résultats obtenus au fil des différentes saisons, au cours desquelles le groupe a aidé les stratèges de

l'armée à se préparer à des formes de conflits qui auraient probablement échappé aux méthodes traditionnelles de prospective. Une quatrième saison est d'ailleurs en cours de production.

Les rapports entre l'armée, la littérature et le cinéma ne sont pas nouveaux, datant pour certains du XIX^{e} siècle. D'aucuns prétendront qu'il s'agit là d'une apologie de la guerre mais, à mon sens, il n'en est rien. Il s'agit au contraire d'un exercice, certes très difficile, d'analyse et d'imagination de notre société, ainsi que des rapports humains et de leur devenir. Chacun se souviendra des fulgurances de René Barjavel, Isaac Asimov ou Philip K. Dick, qui ont parfois pu passer pour de véritables prophéties autour desquelles ont pu être abordées les questions touchant à l'informatique, à l'image, aux robots, à l'impact de la technologie sur le travail, sur l'automatisation de celui-ci, sur la conquête spatiale, sur les conflits, bref, sur la civilisation tout entière. Messieurs, que pensez-vous de ce genre de projets faisant la part belle à l'imagination au service de la prospective ? Comment la gendarmerie appréhende-t-elle le futur du maintien de l'ordre et sa relation aux citoyens à l'égard des évolutions technologiques que nous vivons ? Avez-vous déjà mis en place des outils numériques ou des téléservices visant à vous adapter aux changements sociétaux ?

M. Charles de la Verpillière. Vos exposés liminaires très complets ont déjà répondu à la plupart des questions que nous aurions pu poser. Néanmoins, en ce qui me concerne, il en reste au moins une. On sait depuis l'Antiquité que la guerre est une course-poursuite entre la cuirasse et l'épée. Lorsqu'un inventeur génial, à l'aube de l'humanité, a fabriqué une fronde, un autre tout aussi intelligent a eu l'idée du bouclier. Nos adversaires, c'est-à-dire la délinquance, les milieux radicaux, le terrorisme, sont-ils montés en gamme ? Utilisent-t-ils des technologies de plus en plus pointues ? La menace technologique, d'une façon générale, existe-t-elle de façon spécifique aussi dans le domaine d'action de la gendarmerie ?

M. Christophe Blanchet. Nous vous remercions pour vos interventions qui montrent votre souci d'adaptation constante à la société dans laquelle nous évoluons et votre volonté de faire face aux défis que représente la numérisation des échanges. Votre institution a su s'adapter et s'intéresse à l'espace cyber dans toutes ses dimensions, et ce, de longue date.

Concernant la transformation, je souhaiterais prendre l'exemple de la brigade 4.0 inaugurée en Haute-Saône il y a un peu moins d'un mois. Pour résumer, à la suite de la création d'une nouvelle caserne dans ce département, une ancienne caserne a été dissoute à une quinzaine de kilomètres et a été remplacée par une permanence de trois jours par semaine dans la maison France services et des patrouilles de réservistes. Les plaintes peuvent également être prises au domicile des citoyens. On peut comprendre l'émoi pour la population et les élus locaux face à la disparition de cette caserne. Pourtant, l'attention portée par le Gouvernement à ce sujet semble avoir convaincu. J'aimerais donc connaître vos premiers retours d'expérience à ce sujet.

Comme vous le savez, voir davantage de membres des forces de l'ordre sur le terrain constitue à la fois un engagement du Président de la République et une attente forte des Français. Ainsi, alors que la gendarmerie souhaite recourir à davantage de réservistes, pouvez-vous me dire dans quelle mesure ces derniers sont associés aux réflexions sur la transformation ? Comment imaginez-vous la future gestion des procurations des fameuses tâches indues, qui permettraient peut-être de placer plus de gendarmes sur le terrain ? Dans le rapport que j'ai rendu l'année dernière avec mon collègue Jean-François Parigi, nous avions

souligné la richesse qu'apportent les réservistes à l'institution en termes de transformation. Ces derniers, disposant d'une part d'une expérience dans le secteur civil, voire d'une expertise rare, ont en outre une connaissance de votre institution, de son langage et de ses codes.

Qu'il s'agisse de réservistes ou de gendarmes de carrière, cette ambition de mettre plus de bleu sur le terrain se traduit-elle aussi par l'importance de mettre plus de bleu sur internet ? La création et les objectifs du ComCyberGend ne nous ont pas échappé et celui-ci devra compter à terme 10 000 cyber-enquêteurs. Nous ne pouvons toutefois pas manquer de nous inquiéter au regard de la déconnexion entre la police du web et la population. Les citoyens ont-ils aujourd'hui davantage le réflexe de se tourner vers vous pour rapporter les crimes et délits qui se déroulent en ligne ? Pour mémoire, en 2017, seuls 0,6 % des personnes interrogées savaient à qui s'adresser en cas de problème cyber. Pourtant, nous avons tous eu connaissance ou été confrontés au problème, qu'il s'agisse de contrefaçon ou de cyberharcèlement, et en tant qu'élus, nous sommes nous-mêmes menacés trop régulièrement. Je tiens ainsi à remercier l'ensemble de la gendarmerie pour l'accueil toujours bienveillant à notre égard. Quand on connaît l'ampleur que peut prendre un cyberharcèlement, comme en témoignent l'affaire Mila et l'affaire Shaina, on comprend à quel point ces nouveaux outils peuvent être nocifs. Dès lors, comment envisagez-vous les opérations de communication à destination du public et des jeunes en particulier ?

Pourriez-vous nous préciser également ce qu'est le gilet trois en un ?

Enfin, comment les dix brevets que vous avez déposés sont-ils protégés ? Le dépôt de ces brevets peut-il permettre d'en tirer un bénéfice ?

M. Jean-Charles Larsonneur. Pour répondre à l'évolution des menaces sur le territoire national, il faut d'abord renforcer les effectifs des forces de sécurité intérieure et le député finistérien que je suis se réjouit de constater l'augmentation de ceux-ci dans son département à hauteur de vingt personnels au cours de cette législature. Il s'agit évidemment aussi de renforcer les moyens matériels dont disposent les forces de sécurité, et à l'issue du Beauvau de la sécurité, les crédits d'investissement ont été fortement rehaussés. La prochaine LOPMI devra sanctuariser ces équipements. Mais c'est bien le numérique qui nous réunit aujourd'hui et, à ce titre, l'une des transformations les plus visibles est le terminal NEO Gend. Un plan triennal est programmé pour un marché de renouvellement de la flotte d'environ 100 000 terminaux. Pourriez-vous nous faire un point d'étape sur ce marché, sur les évolutions à venir et peut-être sur son apport au quotidien pour les forces de gendarmerie ?

S'agissant de la brigade numérique, basée à Rennes, composée d'une vingtaine de personnels et accessible sur internet vingt-quatre heures sur vingt-quatre et sept jours sur sept, celle-ci prend désormais en charge la plateforme numérique d'accompagnement des victimes de violences sexuelles et sexistes, de violences conjugales, du cyberharcèlement et des discriminations. Disposez-vous de statistiques sur les demandes quotidiennes en la matière ? Avez-vous observé un surcroît de demandes liées soit au contexte – covid, par exemple – soit à ce nouveau mode d'accès aux services de la gendarmerie ?

J'évoquerai enfin le Centre de lutte contre les criminalités numériques. Dans son rapport budgétaire 2021, notre collègue Xavier Batut indiquait les objectifs en termes d'effectifs fixés par le DGGN, à savoir 7 000 cybergendarmes en 2022, la présence d'antennes du C3N dans chaque région en 2023 et des référents sûreté cyber dans chaque

groupement. Pourriez-vous nous en dire un peu plus sur le déploiement des antennes du C3N en région et, notamment, quelles seront leurs attributions précises et quelle organisation dans le temps est envisagée ?

M. André Chassaigne. Messieurs, je vous remercie vivement de votre présence devant la commission et de vos présentations édifiantes, pétries d'un mot très fort, l'humain, très souvent prononcé.

Le cyber est une nouvelle frontière qui n'a rien à envier au monde physique. Tous les aspects de notre vie quotidienne se retrouvent dupliqués et amplifiés sur internet avec une nette augmentation constatée au cours de la crise sanitaire, au regard des temps d'écran accrus. C'est un fait, vous l'avez dit, la lutte contre la criminalité, les trafics, les escroqueries et le terrorisme se déroulent de plus en plus dans le cyberespace. Personne n'est à l'abri, c'est pourquoi la sensibilisation et l'accompagnement des citoyens par la gendarmerie sont indispensables.

Mais la transformation numérique et la cybersécurité sont aussi une affaire de gouvernance. Les élus locaux, maires et collectivités territoriales, doivent coopérer étroitement avec les gendarmes sur place. Malheureusement, l'action et les moyens s'arrêtent souvent aux grandes métropoles, les petites communes n'étant pas toujours capables de maîtriser ni certains dossiers ni les nouvelles technologies. Il nous faut donc obtenir les moyens qui nous permettent de nous préparer en collaboration avec la gendarmerie, premier service public de proximité sur nos territoires. Les dispositifs de prévention, comme Immunité Cyber, qui encouragent les collectivités à dresser un état des lieux de leur niveau de protection en lien avec l'État et à prendre contact avec la gendarmerie pour obtenir de l'aide, doivent être multipliés.

Ma première question porte sur les synergies entre le privé et le public. Comment assurez-vous une collaboration complémentaire et enrichissante qui ne mène pas à une perte de compétence et de souveraineté de l'État dans le numérique ?

En outre, la gendarmerie recrute désormais 40 % d'officiers à profil scientifique et cyber. Comment pensez-vous attirer l'attention de nos jeunes dans le domaine numérique ?

Finalement, le numérique ne s'arrête pas aux frontières. Quel est, plus globalement, l'état des partenariats numériques et scientifiques au sein de l'Union européenne ? Quel rôle peuvent-ils jouer pour préparer la gendarmerie aux enjeux de demain ?

M. Jean Lassalle. Mes collègues ont décliné l'ensemble de vos qualités et je partage leurs points de vue. Je souhaiterais savoir quel a été le bilan de la convention que vous avez passée avec les missions locales. Il me semble qu'elle constitue une façon à la fois militaire et citoyenne d'intéresser, d'informer et peut-être d'attirer une partie de la jeunesse.

Par ailleurs, à l'aune de tout ce que vous nous avez dit, pensez-vous que nous sommes prêts pour le vote numérique, compte tenu de l'ensemble des dangers que représentent les cyberattaques potentielles ?

Mme Josy Poueyto. Ne peut-on craindre, à terme, un amoindrissement des compétences cognitives de nos hommes, qui pourraient perdre leurs réflexes en recourant

systématiquement à l'intelligence artificielle ? Pire encore, cela pourrait-il menacer leur libre arbitre dans une situation donnée ?

Mme Florence Morlighem. Je vous remercie pour la très grande qualité de vos interventions. Aujourd'hui, tout porte à croire que la prochaine crise sera cyber. La présidence française de l'Union européenne, l'élection présidentielle, la coupe du monde de rugby en 2023, les jeux olympiques de Paris en 2024 sont autant d'événements propices à une importante menace cyber. Il existe donc un réel besoin de coordination et de montée en puissance. Il est très important de sensibiliser les citoyens à l'enjeu cyber et les forums internationaux tels que celui de Lille y contribuent grandement. Pourriez-vous nous apporter un éclairage particulier sur la montée en puissance des réservistes citoyens et opérationnels dans le cadre de votre stratégie cyber ?

Mme Patricia Mirallès. Je souhaite vous remercier pour le soutien que vous apportez aux élus en ces temps difficiles. Quels éléments pourraient vous permettre de mener une action encore plus efficace ?

M. Jacques Marilossian. En 2022, la gendarmerie nationale fête ses 231 ans et sa modernité est pourtant frappante. Sauf erreur de ma part, l'école de gendarmerie de Chaumont a incorporé en septembre dernier une e-compagnie de 112 élèves. L'objectif de cette formation n'est pas d'en faire des spécialistes mais de les former aux technologies les plus modernes pour les répartir ensuite dans des unités traditionnelles de la gendarmerie, en tant qu'ambassadeurs de la culture numérique au sein de ces dernières. Cette e-compagnie sera une première et constitue le début d'un projet qui peut représenter un programme numérique plus important pour la gendarmerie. Elle permettra de faire face aux appels à la violence sur les réseaux sociaux et en particulier ceux menés contre les élus de la République, mais aussi à toutes les manifestations non autorisées ou les préparations d'attentat. Pourriez-vous nous expliquer quelles sont vos attentes liées à cette démarche innovante ?

Mme Carole Bureau-Bonnard. Je souhaiterais évoquer la menace nucléaire, radiologique, biologique et chimique (NRBC). La cellule nationale F2NRBC de Satory, le GIGN et l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) se situent au cœur des réactions face à ces risques. Pourriez-vous nous préciser le rôle du CyberGEND à ce même niveau ?

Mme Monica Michel-Brassart. Le cyberespace est devenu un terrain d'affrontement comme un autre du fait de la mise en données du monde et du déploiement technologique comme l'IA, l'IoT ou la 5G. La maîtrise de la sécurité se trouve donc au cœur de la confrontation des puissances et les États-Unis comme la Chine surclassent les autres en la matière. Pourtant, la France reste aujourd'hui capable de mener des opérations de cybersécurité et de cyberdéfense intégrées aux manœuvres militaires d'ensemble pour répondre aux attaquants informatiques qui mènent des actions d'espionnage, de trafic, de sabotage, voire de désinformation. Je souhaiterais comprendre quel type d'action de cybersécurité et de cyberdéfense notre gendarmerie est capable de mener à ce jour. Par ailleurs, général Perrot, vous avez évoqué la gouvernance en matière d'IA. Pourriez-vous approfondir votre propos ?

M. Jean Lassalle. Monsieur le contrôleur général, j'ai été particulièrement impressionné par votre démonstration sur notre capacité de délégation de nos capacités

cognitives au GPS. Cet exemple très parlant nous permet de comprendre beaucoup de nous-mêmes.

M. le contrôleur général des armées Christophe Jacquot. La question Red Team, qui interroge également nos liens avec les différentes armées et établit un lien entre culture et défense, me passionne personnellement. Il s'avère que j'ai dirigé récemment un établissement de la défense chargé de la culture et des archives, l'établissement de communication et de production audiovisuelle de la Défense (ECPAD). J'ai moi-même assisté en tant qu'observateur, ainsi que mes camarades gendarmes, à la restitution du travail de la Red Team, véritablement passionnant. Votre question s'inscrit tout à fait dans l'actualité et j'ai à ce titre proposé à la DGGN que nous soyons associés au projet non pas seulement en qualité d'observateurs, mais en tant que participants à l'élaboration de scénarios sur les menaces à venir. J'ai été particulièrement frappé par le scénario de mort culturelle, qui impose une réflexion sur le mode d'action de la gendarmerie à échéance de trente ou cinquante ans. Cela recouvre également la question sur la perte potentielle des facultés cognitives des personnels utilisant l'IA. Il s'agit en effet d'une vraie question d'avenir : comment, dans une trentaine ou une cinquantaine d'années, pourrons-nous en lien avec nos forces armées faire face à des mouvements internes, dans le cadre par exemple d'une évacuation de nos ressortissants ? Je vous remercie de nous avoir donné l'opportunité de nous exprimer sur ce sujet.

S'agissant de nos domaines d'action en lien avec la menace technologique, nous nous situons dans une course permanente et les bases fondamentales de la guerre imposent de toujours faire en sorte de prendre l'avantage. Pour vous donner un exemple précis, en collaboration avec Interpol, la gendarmerie a récemment récupéré une importante quantité de données sur EncroChat, réseau crypté plébiscité par les criminels. Nous nous adaptons donc en permanence à l'évolution de la menace et, dans ce cas précis, nous avons pris l'ascendant en investissant le domaine du *darknet*. Demain, nous serons probablement « à la remorque » sur d'autres menaces, mais nous nous adapterons.

Nous n'avons pas encore de retours d'expérience suffisants au sujet de la brigade 4.0 – brigade de gendarmerie à l'ère du numérique et du digital. Il est actuellement question de la création de 200 brigades de gendarmerie dont un tiers mobile, en particulier en milieu rural, dans le cadre de la LOPMI. Actuellement, nous expérimentons en Ardèche le déplacement de gendarmes grâce à deux camping-cars saisis et adaptés à notre activité afin de permettre aux gendarmes d'intervenir dans le milieu rural, sur des marchés ou auprès d'associations. Cela constitue un exemple très concret de ce que pourrait être la gendarmerie du futur. Quoi qu'il en soit, nous affirmons notre volonté stratégique de changer nos modes d'intervention et de nous placer au plus près de la population.

Les réservistes se déclinent en deux groupes : les réservistes opérationnels – qui font l'objet d'un engagement – et les réservistes citoyens. La fidélisation de nos réservistes nous permet de mieux intervenir. Nous les sollicitons de manière régulière au titre d'expertises particulières, ce qui suppose de leur part une certaine disponibilité. Leur participation est essentielle pour nous. Nous réfléchissons actuellement à une évolution de la forme de notre service de la transformation. J'ai ainsi fait appel à deux réservistes, consultants travaillant en liaison permanente avec le secteur privé pour l'un et le secteur public pour l'autre. Les réservistes citoyens constituent quant à eux un vaste vivier, au sein duquel nous essayons de recruter des personnes exerçant des fonctions opérationnelles dans les secteurs public et privé et auprès de qui nous recueillons des avis, même si nous ne pouvons pas les fidéliser comme

dans le cadre d'un contrat de réserve opérationnelle. Dans mon service, j'ai ainsi pris contact avec des directeurs de la transformation au sein de grands groupes de sorte que nous soyons informés sur la façon dont celle-ci fonctionne aujourd'hui chez eux. Cette activité de *think tank* nous procure une aide très concrète répondant à notre objectif d'agilité et aux besoins propres de la gendarmerie.

Nous protégeons les dix brevets que nous possédons selon le même cadre juridique que tout autre brevet de nature industrielle. Nous percevons quelques royalties, peu élevées actuellement car compensant certains frais. Par exemple, peu de pays disposent de laboratoires ADN tels que les nôtres. Nous avons toutefois évoqué avec les industriels la possibilité d'un développement à l'international, ce qui n'exclut pas à l'avenir que nous touchions des redevances. Notre objectif principal reste néanmoins la protection de nos innovations et non la perception de redevances.

Nous avons la volonté non seulement de soutenir les élus, mais aussi de leur proposer un kit ainsi que des conseils en matière de procédures. Nous souhaitons leur prodiguer une formation sur la façon d'accueillir un administré particulièrement mal disposé sans refuser le contact pour autant, et leur proposer un dispositif concret leur permettant de nous prévenir immédiatement, au-delà du système de SMS déjà en place.

La gendarmerie a en fait une histoire vieille de sept siècles. En 1720, Claude Leblanc a développé à l'échelle nationale le modèle des brigades propre à la région parisienne. Aujourd'hui, nous disposons de 3 100 brigades en métropole et 150 outre-mer.

M. le général Patrick Perrot. Je vous suis très reconnaissant pour les remerciements que vous nous avez adressés. Sachez que c'est tout à fait réciproque, ayant rencontré récemment sur le terrain des élus ouverts au numérique.

En prospective, la démarche est souvent incrémentale, c'est-à-dire que l'on part de l'existant en essayant d'anticiper les scénarios probables. L'intérêt d'associer des auteurs de science-fiction dans le cadre de la Red Team réside dans la démarche de rupture proposée par ces derniers. À mon sens, le XXI^{e} siècle, plus que les précédents, s'inscrira dans la rupture.

Nos adversaires montent effectivement en gamme. L'IA doit nous apporter des aptitudes de transformation proactive. Au sein du ministère de l'Intérieur, nous disposons d'une réelle capacité de réaction mais notre ancrage au ministère des Armées nous rappelle aussi la nécessité d'anticiper et de se projeter afin de devancer nos adversaires. Ceux-ci ne sont pas forcément plus intelligents que les précédents mais ils ont toutes les ressources à disposition. De nos jours, tout un chacun peut apprendre à réaliser en une demi-journée des vidéos compromettantes de type *deepfake*. Les outils disponibles étant croissants, la menace à ce niveau le sera aussi. Il a beaucoup été question de fracture numérique, mais il me semble que le numérique est plutôt inclusif. Il permet la persistance des services.

Nous entretenons une forte synergie avec le secteur privé. Nous sommes sollicités au quotidien par des startups et entreprises diverses et nous tentons de promouvoir l'écosystème français et européen, ce qui constitue à nos yeux une vraie plus-value. C'est d'ailleurs l'un des objectifs de notre partenariat au sein du hub France IA.

Le risque d'amoindrissement des compétences cognitives et de perte du libre arbitre dans la capacité de décision existe bel et bien. Nous y ferons face par la formation. L'IA apporte les solutions les plus probables et nous devons enseigner à nos officiers à s'ouvrir à ce qui n'est pas nécessairement probable. En dehors du risque lié à l'utilisation du GPS, on peut citer l'exemple des applications de traduction. Si l'on poursuit sur cette voie, nos connexions neuronales ne se feront plus. Sur le plan professionnel, la situation est identique : nous devons nous entraîner.

Il existe trois types de gouvernance. La première, qui pourrait paraître séduisante à certains, serait une gouvernance citoyenne reposant sur l'*open data* et l'*open source* et dans laquelle chacun s'autogèrerait. Cette situation serait à mon sens inégalitaire puisque tout le monde ne disposerait pas de capacités identiques à exploiter les données. La seconde est celle des GAFA actuelles et futures. Aujourd'hui, ces entités sont en mesure de fixer les règles grâce à leurs capacités de calcul et de stockage et à la *data* que nous leur procurons au quotidien. Cela représente un vrai risque et nous devons veiller de notre côté à monter en compétence pour ne pas céder de terrain, dans le but de protéger les libertés individuelles. Le mode de gouvernance que je privilégierais est celui de l'État, parce que j'ai confiance en la façon dont nous traitons les données à caractère personnel dans le cadre des contrôles auxquels nous sommes soumis. La gouvernance de l'État est aussi la promesse d'une égalité optimale des services rendus aux citoyens.

M. le contrôleur général des armées Christophe Jacquot. Le directeur général m'a demandé il y a quelques mois de lui faire part de réflexions sur notre stratégie numérique. Le service de la transformation est bien placé pour ce faire en raison de nos liens étroits avec la direction interministérielle de la transformation publique, et la direction de la transformation est en quelque sorte la « voix de l'usager » au sein de la direction générale. La direction des opérations et de l'emploi est l'actrice de la doctrine du lien usager. Nous constatons aujourd'hui un usage croissant du numérique. Pourtant, nous éprouvons le besoin de nous pencher sur notre stratégie dite omnicanale, à savoir sur les liens que nous souhaitons privilégier en présentiel, à distance, en mobilité, etc. Ce sont les réflexions que mène la sous-direction de l'emploi des forces au sein de la direction des opérations et de l'emploi. Les personnels du service de la transformation aiguillent donc la stratégie numérique en rappelant constamment le lien à l'usager, qui doit être décliné à travers les différents outils numériques existants sans sacrifier le présentiel, c'est-à-dire le lien direct et physique avec les élus et les citoyens.

M. le colonel Pierre-Yves Caniotti. Il est bien évident que les organisations criminelles s'approprient les technologies numériques afin d'augmenter leur surface d'attaque, de diversifier leurs activités ou de les dissimuler via le chiffrement.

Les atteintes aux personnes et la haine en ligne représentent environ 15 % des faits liés au cyber constatés par la gendarmerie. Cela concerne notamment le cyberharcèlement – injures, diffamations, harcèlement, menaces de mort, diffusions à caractère sexuel, apologie du terrorisme, pédocriminalité, etc.. Il convient cependant de ne pas ignorer l'existence d'un important « chiffre noir », toutes ces atteintes ne remontant pas au niveau de nos services. Ce décalage est aisément observable lorsqu'on évolue sur les réseaux sociaux. Malgré nos nombreuses communications sur le sujet, des efforts conséquents restent à produire.

Le site magendarmerie.fr gère le portail des violences sexuelles et sexistes. Des gendarmes échangent ainsi avec les usagers, victimes et témoins éventuels. En 2021, 2 300 signalements ont été traités via le portail et la brigade numérique. Tous ont fait l'objet de procès-verbaux de renseignements et 8 % ont donné lieu à des interventions de militaires de la gendarmerie ou de fonctionnaires de police immédiatement.

Les 11 antennes du C3N se situent au sein des sections de recherche de la gendarmerie, situées dans les chefs-lieux des juridictions interrégionales spécialisées. Le phasage dans le déploiement des nouvelles antennes répondra à une logique territoriale, en implantant celles-ci dans certaines zones de façon à parfaire notre maillage, ce qui inclut l'outre-mer, et dans des brigades spécialisées, notamment dans les milieux maritime et aéronautique.

Le risque NRBC est pleinement intégré à l'approche de nos missions. Le ComCyberGend dispose ainsi de militaires qualifiés pour évoluer dans des milieux contaminés. Nous réfléchissons par ailleurs à la mise en œuvre de véhicules spécialisés pour pouvoir intervenir au plus près et réaliser des opérations sur le terrain à l'aide d'équipements résilients. Nous participons à des exercices organisés par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) visant spécifiquement à évaluer nos capacités à investiguer sur des scènes de crime contaminées et à réaliser les premières opérations d'analyse en zone contrôlée en soutien immédiat de l'enquête judiciaire. Les capacités du ComCyberGend viennent se combiner avec des capacités rares par ailleurs, comme la cellule NRBC de la gendarmerie. Là encore, les principes militaires de nos engagements s'appliquent.

De nombreux partenariats se sont créés à différents niveaux et notre arrivée prochaine au Campus cyber nous permettra d'en développer davantage. Le ComCyberGend est particulièrement engagé dans des partenariats avec des associations luttant contre la diffusion de contenus illicites et les atteintes aux mineurs sur internet – associations Point de Contact, e-Enfance ou encore Signal Spam. Nous travaillons également en étroite collaboration avec cybermalveillance.gouv.fr, site géré par le groupement d'intérêt public ACYMA. Nous élaborons ensemble des contenus de prévention, de sensibilisation et d'information sur les principales menaces auprès de tous publics – particuliers, collectivités territoriales et acteurs économiques. Nous développons aussi de nouveaux partenariats visant au partage d'informations sur la menace cyber et à la mise en place de modules de formation continue communs avec des partenaires publics français comme européens et des partenaires privés.

Nous communiquons beaucoup sur le recrutement dans le domaine cyber : auprès d'écoles d'ingénieurs, dans des forums métiers et à La Fabrique Défense. Nous co-organisons le forum international sur la cybercriminalité, ce qui nous permet de communiquer sur les carrières et parcours en gendarmerie susceptibles d'intéresser les jeunes diplômés. Nous assurons par ailleurs une présence sur les réseaux sociaux. Nous ne connaissons pas de difficultés de recrutement à l'heure actuelle au regard de nos objectifs.

120 élèves issus de l'e-compagnie de Chaumont sont déjà sortis. Les prochaines sessions se répartiront non plus sur une mais sur trois compagnies. Les militaires qui y sont formés sont compétents pour recueillir des plaintes sur des infractions spécifiques à la cybercriminalité, pour conduire et diligenter les investigations dans des cas ne nécessitant pas

nécessairement l'appui d'unités du CyberGEND et pour mener des analyses techniques de téléphones portables, ce qui s'avère désormais nécessaire dans toute enquête judiciaire.

Sur le plan cyber, nos réservistes opérationnels pourraient être amenés à participer à des opérations de prévention, ce qui est déjà le cas sur certains territoires. Les réservistes ayant un profil très technique peuvent être associés aux unités opérationnelles, comme le C3N. Il paraît assez clair que la prochaine crise sera de nature numérique. Nous avons donc des besoins en gestion de crise. La gendarmerie s'est organisée en conséquence en participant par exemple à l'exercice Piranet et s'est dotée d'un outil de gestion de crise au niveau de notre centre national des opérations, qui permet de suivre des problématiques comme la détection d'une vulnérabilité ou une cyberattaque ayant une incidence potentielle sur notre propre système d'information ou susceptible d'engendrer une crise numérique entravant la sécurité publique. Cette *task force* numérique pourrait tout à fait recevoir des réservistes. Un travail d'identification de ces personnes et de leurs compétences respectives a déjà été réalisé l'an dernier.

Il est également très intéressant de disposer de réservistes citoyens possédant des compétences très diverses dans de nombreux domaines, l'idée étant de les associer à des comités de réflexion en matière de recherches ouvertes sur internet, de problématiques juridiques, d'états de la menace ou encore d'ouverture à de nouveaux partenariats. Nous souhaitons réellement nous appuyer sur leurs capacités de prospective.

Mme la présidente Françoise Dumas. Vous nous avez démontré combien la gendarmerie est passionnée et nous vous faisons part de notre gratitude et de notre respect. Je retiendrai votre formule, Monsieur le contrôleur général : « celui qui sait est celui qui fait ». Vous savez parfaitement vous adapter aux changements humains, y compris lorsque ceux-ci sont déviants. Ce dernier cycle de la commission nous permet de rendre hommage à nos militaires, qui en éprouvent un réel besoin.

*

* *

La séance est levée à dix-heures cinquante-cinq.

*

* *

Membres présents ou excusés

Présents. - M. Jean-Philippe Ardouin, Mme Françoise Ballet-Blu, Mme Sophie Beaudouin-Hubiere, M. Christophe Blanchet, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. André Chassaigne, M. François Cormier-Bouligeon, Mme Catherine Daufès-Roux, M. Rémi Delatte, Mme Marianne Dubois, Mme Françoise Dumas, M. Olivier Faure, M. Yannick Favennec-Bécot, M. Jean-Marie Fiévet, M. Claude de Ganay, Mme Séverine Gipson, M. Fabien Gouttefarde, Mme Marie Guévenoux, M. Jean-Michel Jacques, M. Loïc

Kervran, Mme Anissa Khedher, M. Jean-Charles Larsonneur, M. Jean Lassalle, M. Didier Le Gac, M. Gilles Le Gendre, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Gérard Menuel, Mme Monica Michel-Brassart, Mme Patricia Mirallès, Mme Florence Morlighem, Mme Josy Poueyto, Mme Catherine Pujol, M. Bernard Reynès, M. Benoit Simian, Mme Laurence Trastour-Isnart, Mme Alexandra Valetta Ardisson, M. Charles de la Verpillière, M. Stéphane Vojetta

Excusés. - M. Florian Bachelier, M. Olivier Becht, M. Jean-Pierre Cubertafon, M. Richard Ferrand, M. Stanislas Guerini, M. David Habib, Mme Manuéla Kéclard-Mondésir, M. Bastien Lachaud, M. Jean-Christophe Lagarde, M. Philippe Meyer, M. Patrick Mignola, M. Gwendal Rouillard, Mme Isabelle Santiago, Mme Nathalie Serre, M. Thierry Solère, M. Joachim Son-Forget, M. Aurélien Taché, M. Stéphane Trompille