ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission d'enquête sur la situation, les missions et les moyens des forces de sécurité, qu'il s'agisse de la police nationale, de la gendarmerie ou de la police municipale

Mercredi
6 mars 2019
Séance de 16 heures 15

Compte rendu n° 2

SESSION ORDINAIRE DE 2018-2019

Présidence de M. Jean-Michel Fauvergue, *Président*

ASSEMBLÉE NATIONALE

La commission d'enquête sur la situation, les missions et les moyens des forces de sécurité, qu'il s'agisse de la police nationale, de la gendarmerie ou de la police municipale auditionne M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.

M. le président Jean-Michel Fauvergue. La commission d'enquête sur la situation, les missions et les moyens des forces de police commence aujourd'hui ses travaux. À l'occasion de cette première audition, nous aborderons avec Thierry Delville les enjeux majeurs de technologie et de cybersécurité qui mobilisent toujours davantage les forces de sécurité intérieure.

Les auditions de notre commission sont publiques, ouvertes à la presse, diffusées en direct sur un canal de la télévision interne et consultables en vidéo sur le site Internet de l'Assemblée nationale.

Conformément aux dispositions de l'article 6 de l'ordonnance du 17 novembre 1958 relatif aux commissions d'enquête, M. Thierry Delville prête serment.

M. Christophe Naegelen, rapporteur. Monsieur Delville, notre commission souhaitait vous auditionner à plusieurs titres : en tant qu'ancien commissaire de la police nationale, mais aussi, et surtout, en tant qu'ancien chef du bureau des systèmes d'information à la direction centrale de la sécurité publique (DCSP). Vous êtes notamment à l'origine de la création du service des technologies et des systèmes d'information de la sécurité intérieure. Cet aspect nous intéresse tout particulièrement, d'autant qu'il est partagé entre la gendarmerie nationale et la police nationale. Notre commission d'enquête porte sur ces deux forces, et aura à cœur d'explorer des pistes de travail communes à leur égard.

En 2009, vous avez pris la direction des services techniques et logistiques de la préfecture de police de Paris. Puis vous avez été nommé délégué interministériel aux industries de sécurité, en 2014, avant de voir vos prérogatives s'étendre en 2017 à la lutte contre les cybermenaces.

Au vu des menaces qui nous guettent, nous savons l'importance que revêtent la cybersécurité et les équipements de nos forces de sécurité. Quels enseignements avez-vous tirés de vos différentes expériences, et comment envisagez-vous l'avenir des cybermenaces et de la cybertechnologie ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Je vous remercie de m'inviter à témoigner sur un sujet qui m'est particulièrement cher. En effet, si, après trente-deux ans passés au sein de la police nationale, j'ai décidé depuis peu de relever un nouveau défi dans le secteur privé, le sujet des moyens d'action et de l'organisation des forces de sécurité me tient toujours particulièrement à cœur.

Je tiens à saluer l'initiative de cette commission, tant j'ai regretté, ces dernières années, que la sécurité soit le plus souvent abordée en réponse à des événements d'actualité, sur des périmètres restreints et des thématiques précises – le terrorisme au premier chef. J'espère sincèrement qu'en témoignant devant votre commission, je contribuerai à vous convaincre de la nécessité d'engager une véritable démarche stratégique sur la sécurité

intérieure, à l’image des lois de programmation militaire qui apportent de la visibilité aux orientations et à l’action du pays en matière de défense.

Mon expérience et ma carrière dans la police m’ont conduit à exercer divers métiers, dans des commissariats de la banlieue parisienne, à la direction centrale de la sécurité publique puis à la tête d’un service en charge des technologies et de la recherche dans la police nationale. Notez qu’à l’époque, le service des technologies et des systèmes d'information de la sécurité intérieure n'était pas encore fusionné avec la gendarmerie.

J’ai ensuite pris la tête d’une structure opérationnelle assez atypique, la direction des services techniques de la préfecture de police de Paris, qui remplit une mission essentielle de soutien traditionnel aux forces. Comme l’affirmait un de mes prédécesseurs, la logistique est le premier temps de l’action !

Enfin, j’ai été chargé d’une délégation dont le champ s’est progressivement étendu des industries de sécurité à la lutte contre les cybermenaces. L’un de nos actes importants fut la création d’une filière industrielle de sécurité, qui prend désormais la forme d’un comité stratégique – ce dont je me réjouis. Je me suis également attaché à coordonner et à animer le réseau des acteurs de la cybersécurité pour le ministère de l’intérieur : policiers, gendarmes, direction générale de la sécurité intérieure (DGSI) et acteurs de la protection des infrastructures du ministère, sous l’autorité du haut fonctionnaire de défense.

Cette alternance de postes revêtant des dimensions opérationnelles, managériales et stratégiques m’a permis de travailler avec l’ensemble des acteurs du ministère, dans la diversité de leurs cultures, leurs histoires et leurs organisations. J’ai pu mesurer combien ce ministère et ses personnels étaient essentiels à notre société et méritaient une attention particulière. Vous y répondez aujourd'hui fort opportunément.

Ayant quitté mes fonctions il y a plus de quatre mois, je ne saurais vous communiquer des données chiffrées actualisées. Mon témoignage sera celui d’un policier ayant commencé sa carrière il y a un peu plus de trente ans comme inspecteur de police doté de quelques compétences informatiques. J'ai suivi un parcours assez atypique, à une époque où la police ne comptait pas de filière technologique et informatique. Après avoir passé le concours des commissaires, j’ai assez rapidement pris la direction des services actifs de la police nationale. À ce titre, j’ai eu le plaisir et l’honneur de participer à des travaux qui se sont avérés importants pour la sécurité ces quinze dernières années. C’est ainsi que, pour la première fois, le ministère de l’intérieur a été associé aux travaux du Livre blanc sur la défense et la sécurité nationale de 2008. Nous avons reconduit l’exercice en 2013. J’ai également participé à des travaux ayant nourri le Livre blanc sur la sécurité intérieure, commandé par le ministre de l’intérieur en 2011. En 2014, j’ai piloté plus directement des travaux diligentés par le ministre dans le cadre du plan de modernisation de la sécurité intérieure, qui comportait une dimension technologique très marquée. J’ai conduit des travaux du même ordre sollicités en 2016 par M. Cazeneuve, ayant permis de recenser les besoins des forces de police et de gendarmerie, ainsi que des services de renseignement et de la sécurité civile.

Il y a treize ans, j’ai été chargé de mettre en place le service des technologies et des systèmes d'information (STSI), créé par le ministre de l’intérieur en février 2005. Il m’a été demandé, dans ce cadre, de faire passer la police d’une entreprise de main-d’œuvre à une entreprise de haute technologie – ou, en tout cas, d’aider la police à accompagner le basculement de la société dans le numérique. Beaucoup a été fait à ce titre, bien que la

situation budgétaire ne soit guère propice à un travail sur les enjeux de modernisation. Un très net déséquilibre persiste en effet entre l'enveloppe couvrant la masse salariale des forces de sécurité – police et gendarmerie – et les crédits de fonctionnement et d'investissement. En 2005, sur le périmètre de la police, la masse salariale représentait 87 % du budget. Il est fort probable qu'aujourd'hui, elle en atteigne 90 %. Les moyens pouvant être alloués aux investissements s'en trouvent réduits.

Pour autant, de nombreux efforts de mutualisation et de rationalisation ont été accomplis ces dernières années. Citons en particulier le rapprochement du système de traitement des infractions constatées (STIC) et du système judiciaire de documentation et d'exploitation (JUDEX), ayant donné naissance au fichier de traitement d'antécédents judiciaires (TAJ) partagé par la police et la gendarmerie. S'y sont ajoutés des travaux de modernisation en matière de police technique et scientifique.

Il reste beaucoup à accomplir. Parmi les principaux enjeux figure le remplacement des réseaux radio, qui représentera un coût majeur dans les années à venir. Déjà, la mise en place de ces réseaux il y a près de deux décennies avait nécessité un investissement considérable. Un autre sujet me tient particulièrement à cœur et mérite de progresser, au-delà des actions déjà engagées : le rapprochement des plateformes d'appel d'urgence. C'est un élément important du service rendu aux citoyens, dont ont su s'emparer une dizaine de pays européens.

Enfin, des travaux restent à conduire sur l'utilisation du numérique, en veillant à articuler les dimensions légale et réglementaire avec l'acceptabilité sociale de cette technologie. Je pense ici à l'utilisation d'informations numériques en source ouverte pour des travaux de renseignement territorial, ou encore à l'exploitation de sources vidéo. Les nombreux outils qui sont disponibles dans ces domaines ne sont pas sans soulever des interrogations légales et sociales. Ils méritent de faire l'objet d'un débat et d'être inscrits dans une démarche stratégique.

J'en viens à la montée en puissance des cybermenaces. J'ai été en charge de ces questions ces trois dernières années au ministère de l'intérieur, sous l'angle de la coordination mais sans exercer de fonction opérationnelle. En la matière, chaque direction générale gère les activités et les affaires qui lui sont propres, en relation, notamment, avec le ministère de la Justice. L'État français a réagi vite et bien à l'essor des cybermenaces. Il a su structurer un modèle qui suscite un intérêt à l'échelle internationale. En revanche, il reste à progresser dans la déclinaison concrète de ces sujets au sein des services de police et de gendarmerie au quotidien. J'y ai consacré une feuille de route, qui a d'ailleurs été mentionnée lors d'un récent forum à Lille par le secrétaire d'État auprès du ministre de l'intérieur, Laurent Nuñez. Elle invite à se saisir des enjeux de cybersécurité sous l'angle de la formation des personnels, du recrutement de spécialistes ou encore du renforcement des structures d'enquête.

Je me contenterai d'une statistique pour illustrer l'ampleur que prend la cybercriminalité. Il y a deux décennies, notre pays recensait plus d'un millier de braquages de banques chaque année, et infiniment peu d'atteintes à l'espace cybernétique. Aujourd'hui, les braquages ne dépassent guère la centaine, tandis que 1,2 million de foyers font l'objet d'un usage frauduleux de leur carte bancaire. Le ministère de l'intérieur doit se dimensionner pour faire face à cette déferlante. Au-delà de l'exemple que j'ai cité se présentent d'autres enjeux, notamment d'accompagnement du tissu économique – et tout particulièrement des petites et moyennes entreprises, qui sont insuffisamment protégées contre les cybermenaces.

M. le président Jean-Michel Fauvergue. Bien que les ressources mobilisables à cet effet ne représentent que 10 % du budget du ministère, de grands projets technologiques ont-ils été ou sont-ils envisagés ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. À ce jour, le projet technologique le plus structurant touchant les forces de l'ordre reste le déploiement du réseau radio numérique entre le début des années 1990 et 2007. Ce réseau est en quelque sorte la « colonne vertébrale » des acteurs de terrain, pour lesquels la coupure des communications avec la salle de commandement présenterait un réel danger. Il importe désormais de moderniser et de renouveler ces technologies, en s'appuyant sur des capacités nouvelles. Les capacités de transmission de ce réseau sont insuffisantes – elles sont nettement inférieures à celles qu'offre le moindre téléphone mobile. Il faudra tirer parti de la 5G pour permettre aux forces de l'ordre de transmettre des données volumineuses, notamment des vidéos, de façon sécurisée. Ces infrastructures doivent être résilientes : elles doivent continuer à fonctionner quand tous les autres dispositifs ont été atteints ; d'où leur coût important. Tel est, à mes yeux, l'investissement prioritaire. Cet enjeu est bien identifié par le ministère, et formalisé dans le cadre du projet « réseau radio du futur ».

D'autres projets sont en cours, comme la numérisation de la procédure pénale, c'est-à-dire le stockage des informations pénales sur des durées longues, et la facilitation des recherches.

Plutôt que de se livrer à une course sans fin aux nouveaux outils, il me paraît indispensable de consolider les infrastructures : le câblage doit être modernisé dans les commissariats, et les moyens de transmission doivent être actualisés. Les dispositifs de stockage de l'information doivent en outre être chiffrés et sécurisés de façon renforcée, pour résister à de potentielles attaques informatiques. J'estime que des moyens devraient être consacrés prioritairement à ces sujets.

M. le président Jean-Michel Fauvergue. J'invite nos administrateurs, que je remercie pour leur travail et leur disponibilité, à collecter auprès du ministère de l'intérieur l'ensemble des travaux ayant été menés dans ces domaines, en particulier par Thierry Delville.

M. Christophe Naegelen, rapporteur. En 2018, il avait été envisagé de créer une grande direction du numérique au sein du ministère de l'intérieur, fusionnant la direction des systèmes d'information et de communication avec les services homologues de la préfecture de police et de la direction générale de la sécurité civile et de la gestion des crises. La question s'était posée d'y intégrer ou non le STSI. Monsieur Delville, quel est votre point de vue sur le sujet ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Ces travaux se poursuivent. Ayant quitté mes fonctions il y a plusieurs mois, je ne pourrai vous informer de leurs derniers développements. Je vous livrerai néanmoins ma vision de ce projet, dont j'ai d'ailleurs fait état avant mon départ.

L'enjeu de la transformation numérique doit être porté de manière unitaire. Si le STSI a été créé en 2005, c'est parce qu'à l'époque, la police nationale était insatisfaite de la manière dont étaient gouvernés les crédits. Nous étions avant l'entrée en vigueur de la loi organique relative aux lois de finances (LOLF), dans un modèle où les directions

opérationnelles – la direction générale de la police nationale (DGPN), en l'espèce – n'avaient pas de visibilité sur les projets et les programmes. Il en va autrement depuis la LOLF, et nous ne pouvons que nous en réjouir. Il serait néanmoins souhaitable que les compétences, les ressources et la vision touchant aux questions technologiques fassent l'objet d'une gouvernance unifiée et renforcée au sein du ministère, qui puisse contribuer à une transformation culturelle.

J'ai intégré cette administration il y a plus de trente ans en tant qu'inspecteur de police, après avoir passé un concours comportant une option informatique. Je doute que cette option existe encore. C'est pourtant un véritable enjeu. *A contrario*, la gendarmerie compte une filière technologique dans laquelle elle recrute des diplômés de niveau élevé, y compris des polytechniciens. Elle accompagne tout au long de leur carrière ces hauts potentiels, susceptibles de devenir responsables de la police technique et scientifique ou de services de cybersécurité.

Je souhaiterais que dans la conduite des projets, indépendamment des grands pôles – DGPN, direction générale de la gendarmerie nationale (DGGN), secrétariat général… –, il y ait toujours à la table du ministre de l'intérieur un acteur, au service de tous les autres, qui porte le sujet de la modernisation et de la transformation numérique.

Le ministère de l'intérieur a besoin d'une grande direction générale du numérique, tant pour sa propre transformation que dans le cadre de ses relations avec d'autres acteurs interministériels tels que la direction générale de l'armement ou le secrétariat général de la défense et de la sécurité nationale (SGDSN). Telle est ma conviction personnelle.

M. Christophe Naegelen, rapporteur. Le STSI devrait-il, selon vous, y être inclus ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Naturellement. Il est même possible d'aller plus loin. J'ai été en charge, à Paris, d'une direction qui regroupait des compétences de la direction des systèmes d'information de la préfecture de police, des services logistiques et de divers services de support opérationnel. Dans un même esprit, une grande direction du numérique du ministère de l'intérieur, si elle voyait le jour, ne devrait pas être éloignée des enjeux d'équipement des forces. Bien souvent, ces aspects sont liés. Les dispositifs de protection des agents ou d'armement intègrent tous des technologies, à de rares exceptions. Au-delà d'une direction numérique, il conviendrait ainsi de réfléchir à une direction support de la transformation et de la modernisation.

M. le président Jean-Michel Fauvergue. Il s'agirait donc d'une direction support pour toutes les unités de sécurité intérieure, qui interviendrait aussi bien en matière de numérique que d'équipements. Y incluriez-vous les équipements roulants ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Oui. Comme j'ai pu en faire l'expérience à la direction des services techniques, le coût d'une voiture de police, tel qu'il est négocié avec le service des achats, double sous l'effet des technologies que l'on y intègre : rampe accueillant le dispositif de reconnaissance de plaques minéralogiques et la caméra, radio, etc. Le véhicule doit être considéré comme un outil technologique supplémentaire, mobile et extrêmement coûteux.

M. le président Jean-Michel Fauvergue. Quel serait le positionnement optimal de cette direction ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. J'en ferais une direction générale qui traiterait quotidiennement avec le ministre ou son directeur de cabinet, au même titre que les autres directions générales.

Mme Nicole Trisse. Vous semblerait-il nécessaire de repenser la formation dans les écoles de police afin qu'elle intègre la dimension numérique ? De nouveaux critères de recrutement s'imposent-ils ? Est-il souhaitable de former aux technologies numériques les agents en fonction depuis quelque temps ? Si oui, est-ce prévu ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Ma réponse sera parcellaire, car je ne suis pas entré dans un niveau de connaissance précis de la formation dans chaque direction générale. Je ne saurais comparer, par exemple, l'effort de formation rempli par la DGSI et la DGGN.

Cependant, la police nationale me semble devoir réaliser un effort tout particulier pour élargir le champ de compétence de ses recrues. Il est certes important de connaître le droit pénal et le droit administratif pour passer un concours, mais ces disciplines peuvent aussi s'acquérir à l'issue du recrutement. Pourquoi un candidat ayant une formation d'ingénieur ne pourrait-il pas se présenter aux épreuves ? Il arrive que de tels profils passent le concours de commissaire, mais ils intègrent ensuite rarement les services technologiques. Il me paraît donc prioritaire d'ouvrir les concours.

Par ailleurs, il est absolument essentiel de renforcer la formation à la cybersécurité, par des dispositifs qu'il appartient aux spécialistes de la pédagogie de définir : modules à distance, sessions sur site... De même que les experts-comptables se forment régulièrement aux normes IFRS, les forces de sécurité doivent se voir proposer des dispositifs de formation itératifs leur permettant de maintenir à niveau leurs connaissances et de rendre un service pertinent aux usagers.

Lors des attentats de 2015, nous avons mesuré combien il était important de rencontrer les grands acteurs de l'Internet. Bernard Cazeneuve, alors ministre de l'intérieur, s'était rendu dans la Silicon Valley pour discuter de modalités de coopération. Ce travail a fait l'objet d'un suivi et s'est élargi à d'autres thématiques. Ainsi, des discussions sont en cours à Bruxelles sur le retrait, dans des délais extrêmement courts, de contenus terroristes publiés en ligne. Préalablement, l'une des toutes premières actions entreprises fut de former massivement des correspondants à adresser des réquisitions aux opérateurs, selon des modalités harmonisées mais en tenant compte de la spécificité de chaque acteur. Ceci nécessite un important effort de formation des enquêteurs, et plus encore d'actualisation des connaissances dans la durée, afin de faire face à des phénomènes en évolution constante.

M. Rémi Delatte. Le numérique offre des opportunités, mais présente aussi des risques en concentrant des données sensibles sur un même site. Vous évoquiez la nécessité de se doter d'outils résilients, garantissant une totale sécurité. Or le risque zéro n'existe pas, qui plus est dans un monde où la technique évolue à grande vitesse et où la cybercriminalité a souvent un temps d'avance. Le risque que j'évoque est d'autant plus prégnant que les données sont partagées sur l'ensemble du territoire français – via l'outil NeoGend notamment. Comment s'assurer de la résilience et de la sécurité d'un tel dispositif ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Le risque zéro n'existe pas, en effet, en particulier face aux

cybermenaces. Il faut avoir l'humilité de reconnaître que l'expertise que l'on croit détenir est frappée d'obsolescence en quelques heures, au mieux en quelques jours. Dans les entreprises, les responsables de la sécurité des systèmes d'information sont submergés quotidiennement de failles nécessitant la mise à jour de programmes. Imaginez l'ampleur de la tâche dans de grandes banques ou organisations, où les systèmes d'information sont souvent complexes et résultent de fusions d'entités. Un travail colossal de construction et d'homogénéisation des systèmes doit être mené. Ces enjeux sont tout aussi importants au ministère de l'intérieur. Ils font l'objet d'un suivi scrupuleux, avec la collaboration et la supervision essentielles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). La solution Neo a d'ailleurs été bâtie avec des systèmes d'exploitation fournis et mis à niveau par l'ANSSI. Les préoccupations de sécurité sont donc centrales dans tous les projets.

M. Jean-Louis Thiériot. Vous jugez nécessaire d'établir une programmation pluriannuelle de la sécurité intérieure, portée par une vision à long terme. À cet égard, vous paraîtrait-il opportun d'élaborer un livre blanc de la sécurité intérieure, qui nous permette de poser, dans la durée, les ambitions de sécurité et les moyens afférents ?

Par ailleurs, où en est la filière des entreprises technologiques de sécurité ? Si l'État n'a pas pour vocation première de la porter, il peut néanmoins participer à son développement. Comment agir en ce sens ?

Enfin, vous avez souligné la nécessité de se doter d'un numéro d'appel d'urgence unique. Ayant été président de conseil départemental, j'ai été conduit à réfléchir sur ce sujet. Je me suis notamment intéressé au projet NexSIS développé par les pompiers. Si nous nous dirigions vers un numéro d'appel unique, quelles entités devraient être réunies, et quel acteur serait le plus à même d'en être l'opérateur ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Je suis intimement convaincu qu'une programmation à long terme est nécessaire. Au cours de ma carrière au ministère de l'intérieur, j'ai eu à connaître la loi relative à la modernisation de la police nationale de 1985, puis la première loi d'orientation et de programmation pour la sécurité intérieure de 2002, qui comportait un volet technologique. De nombreux projets en ont découlé. À chaque fois, néanmoins, il s'agissait de « coups », après quoi le sujet restait en sommeil une décennie. On qualifie parfois le ministère de l'intérieur de « ministère de l'urgence ». Il lui manque une programmation de long terme. Les travaux auxquels j'ai contribué s'inscrivaient dans une temporalité de cinq ans, à l'instar de la loi de programmation militaire. Il est nécessaire qu'à leur issue soient effectués un bilan, un contrôle et une évaluation, afin de pouvoir enchaîner sur la loi suivante. Malheureusement, la France ne procède pas à cet exercice en matière de sécurité.

À l'heure où l'on parle de révision constitutionnelle, j'aimerais également que la sécurité fasse l'objet d'une commission spécifique au Parlement, afin que celui-ci bâtisse une expertise pérenne dans ce domaine et qu'il l'applique au contrôle et à l'exécution des lois. Une commission sur la sécurité intérieure, voire sur la sécurité intérieure et la justice, représenterait une avancée considérable pour développer l'expertise et le contrôle du Parlement sur ces sujets.

J'ajoute que les lois de programmation n'ont pas vocation à répondre à des événements dans l'urgence, mais à tracer une vision sur des projets au long cours. Le réseau de radio Acropol a par exemple mis quinze ans à se déployer sur le territoire. Paris accueillera

les Jeux olympiques (JO) en 2024. Nous devrons être à l'heure de cet événement en matière de sécurité. Une loi pourrait viser ce terme.

Il est important que l'État s'implique dans les travaux des filières. Avec l'aide précieuse de Patrick Guyonneau, j'ai eu le plaisir de fonder en octobre 2013 le comité de la filière industrielle de sécurité (COFIS), qui a accédé il y a quelques mois au rang de comité stratégique. La sécurité est ainsi reconnue comme une filière à part entière, et est placée à ce titre sous la coordination du ministère de l'Économie et des Finances. Le ministère de l'intérieur doit absolument y jouer un rôle, comme il l'a fait ces cinq dernières années. Le premier comité de pilotage de la filière fut d'ailleurs coprésidé, en décembre 2015, par le ministre de l'intérieur, Bernard Cazeneuve, et le ministre de l'économie, de l'industrie et du numérique, Emmanuel Macron. Malheureusement, cette instance n'a pu se réunir à nouveau, l'événement ayant été plusieurs fois reporté.

En France, la filière de la sécurité représente 130 000 à 140 000 emplois industriels directs. Si l'y on ajoute les emplois indirects dans les secteurs public et privé, elle dépasse le million d'emplois. Son chiffre d'affaires atteignant 24 milliards d'euros en 2017, et était réalisé pour plus de la moitié à l'export. Il s'agit d'un secteur extrêmement dynamique, en très forte croissance. À la différence des entreprises de sécurité privée traditionnelles, fondées sur la ressource humaine, l'industrie de sécurité produit des solutions technologiques, orientées en particulier vers la cybersécurité et la sécurité physique et logique. L'État n'en est pas le premier acheteur. Le ministère de l'intérieur ne représente que 4 % ou 5 % des ventes réalisées sur le marché domestique. *A contrario*, le ministère des Armées est le client exclusif de la filière de l'armement, hors exportations. Cela constitue une différence majeure. La sécurité doit être pensée, aujourd'hui, dans le cadre de partenariats avec le monde privé. La vision stratégique et l'élaboration éventuelle de lois de programmation ne sauraient éluder cette dimension.

J'en viens au projet de numéro d'appel d'urgence unique, le 112 unifié, qui est envisagé depuis une décennie. Dix à douze États membres se sont dotés d'un tel dispositif. Les départements prennent des initiatives en ce sens. Il reste à savoir comment mettre en œuvre des plateformes comparables à celles de nos voisins, et comment les harmoniser. Je ne saurais dire à qui devrait en être confié le pilotage. La délicate détermination de la gouvernance du dispositif est d'ailleurs l'un des freins du projet. Dans les départements, une autorité s'impose quoi qu'il en soit, le préfet. Il suffirait qu'une décision soit prise sur le pilotage d'une plateforme d'urgence dédiée à la réponse aux citoyens, pour que tous les acteurs se mettent en ordre de marche.

M. Jean-Claude Bouchet. Nous savons tous que pour être efficaces, les forces de sécurité, quelles qu'elles soient, ont besoin de moyens : véhicules, armement, réseaux radio, etc. Or les infrastructures de communication sont fragiles : il suffit de couper une fibre ou de faire tomber une antenne pour les mettre hors d'usage. Dans certains commissariats, les infrastructures ont quinze ans de retard. Quel budget serait nécessaire pour les mettre à niveau ?

Par ailleurs, les moyens dont nous disposons en matière de cybersécurité permettent-ils de contrer les attaques et de mener des enquêtes efficaces ? Sont-ils suffisants, sachant que, dans ce domaine, les criminels ont toujours un temps d'avance sur la technologie ? Des comparaisons internationales permettent-elles de juger si la France est au niveau en la matière ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. C'est un exercice difficile que de déterminer le budget de mise à niveau des infrastructures. Le projet de plan de modernisation de la sécurité intérieure, remis peu avant la dernière élection présidentielle, comportait plus de 70 pistes d'action, dont beaucoup portaient sur les infrastructures. Il évaluait le budget global nécessaire entre 2 et 2,5 milliards d'euros sur cinq ans, la moitié environ correspondant aux infrastructures, et préconisait le renforcement des effectifs à hauteur de 300 à 400 agents techniques. Beaucoup a été entrepris, grâce aux efforts des directions générales et à un abondement budgétaire. Je ne suis pas en mesure de dire ce qu'il reste à faire. Je ne suis pas certain, toutefois, que les infrastructures soient priorisées dans ce cadre. Elles méritent pourtant une attention particulière. La modernisation et la sécurisation des infrastructures de réseau – radio et informatiques – nécessiteraient un investissement de l'ordre d'un milliard d'euros sur cinq ans.

Je n'ai pas le sentiment que la France accuse un retard en matière de cybersécurité. J'ai participé aux travaux menés il y a un an par le SGDSN avec l'ANSSI, dont a découlé la revue stratégique de cyberdéfense. Notre principal enjeu fut de convaincre les différents acteurs de la nécessité de travailler ensemble. Des avancées importantes ont été réalisées dans la gouvernance des sujets de cybersécurité. L'ANSSI, dirigée par un homme remarquable, Guillaume Poupard, assure une animation et une coordination des acteurs sous l'autorité du SGDSN. Nous disposons donc d'une organisation intégrée et interministérielle. Si les parties ont parfois des vues divergentes, elles s'accordent sur la nécessité de mener certains travaux : formation, actualisation permanente des capacités face à une cybercriminalité en évolution constante, etc.

Les pratiques de cybercriminalité se sont considérablement transformées, ne serait-ce que depuis 2015. Le *darknet* est devenu une terre promise pour les mafieux et cybercriminels de tous ordres. Un rapport publié il y a un peu plus d'un an faisait état de 100 000 téléchargements d'outils permettant d'accéder à ce réseau. Les forces de sécurité doivent se mettre en capacité de tracer ces outils, qui évoluent constamment, pour mener le travail d'investigation nécessaire. À ce volet judiciaire s'ajoute celui du renseignement, à une granularité toute particulière. Tout ceci a un coût considérable.

Mme Agnès Firmin Le Bodo. Vous avez insisté sur la mutualisation des efforts et la nécessaire co-construction des projets. La localisation sur un même site de l'ANSSI et du centre d'analyse de lutte informatique défensive doit produire ses effets. M. Poupard fait état d'une difficulté à recruter des ingénieurs spécialisés en cyberattaque ou en cyberdéfense. Quand la France développera-t-elle véritablement cette spécialité, pour se doter des compétences dont elle a besoin ?

S'agissant des infrastructures, il convient de rappeler que certains commissariats n'ont pas même une connexion Internet satisfaisante. J'ose espérer que nos futurs policiers seront formés aux technologies. Qu'en est-il de la formation continue des agents en place, qui paraît absolument nécessaire ? La cybersécurité se vit en effet au quotidien.

Enfin, monsieur Delville, vous avez enfin évoqué les jeux olympiques. Dans cette perspective, comment la France peut-elle renforcer ses capacités de cyberprévention, afin d'en faire un axe de défense et de cybersécurité ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. L'effort de modernisation des infrastructures que j'ai

mentionné inclut les commissariats et les brigades de gendarmerie sur l'ensemble du territoire.

Les ingénieurs en cybersécurité sont une denrée rare et très recherchée. Je rencontrais aujourd'hui même le directeur d'une école d'ingénieurs de la région parisienne, avec lequel j'explore des pistes pour identifier des profils atypiques.

J'aime citer à ce propos une anecdote particulièrement éclairante. Elle nous renvoie en 1988, lorsque j'étais affecté aux activités micro-informatiques de la direction des transmissions et de l'informatique – devenue depuis la direction des systèmes d'information et de communication (DSIC). À l'époque, les ordinateurs commençaient à peine à se doter de disques durs. L'un de nos agents les plus brillants en développement micro-informatique était un gardien de la paix. Jusque-là chauffeur au service central automobile, il avait été repéré car il développait en hexadécimal à ses heures perdues – autant dire qu'il était capable d'entrer dans les profondeurs de la machine. Nous étions en charge du suivi des résultats lors des soirées électorales. Le système principal était confié à un important industriel, qui faisait le lien entre les préfectures et le ministère de l'intérieur. Notre gardien de la paix avait pour sa part développé un réseau de secours. Un soir d'élection où le ministre a demandé une représentation des résultats dans un format non prévu par le prestataire, celui-ci s'est montré incapable d'y répondre. Il n'a fallu qu'une demi-heure à mon collègue gardien de la paix pour concevoir une solution *ad hoc*.

Les acteurs de la cybersécurité ont conscience qu'ils ont intérêt à offrir une deuxième chance à des talents qui n'ont suivi les cursus traditionnels. Je pense notamment à des jeunes diplômés d'écoles de commerce, qui ne s'épanouissent pas dans les affaires mais possèdent des bases mathématiques. Je pense aussi à des personnes qui ont pris des chemins tout autres, mais qui ont une appétence particulière pour l'informatique. Des initiatives commencent à apparaître pour tirer parti de ces talents.

Au-delà de la formation, l'enjeu majeur sera de fidéliser ces professionnels. Nul doute, en effet, qu'ils seront démarchés par des acteurs privés capables de leur proposer des rémunérations alléchantes.

Une mise à niveau des personnels est de surcroît nécessaire, via la formation continue. Il faut faire l'effort d'extraire des agents de leur activité quotidienne pour les inscrire dans des cycles longs de formation. C'est d'ailleurs l'occasion de faire monter en gamme et de réorienter des personnels – sachant que quiconque entre désormais sur le marché du travail est appelé à exercer trois ou quatre métiers.

Les JO ont pour partenaire informatique un porte-drapeau de l'industrie et de l'expertise françaises. Un écosystème est en train de se mobiliser dans le cadre de la filière, dans la perspective des JO de Paris en 2024. Ces jeux devront être une réussite en termes d'innovation et de démonstration de notre savoir-faire. Selon qu'elles se sont tenues à Londres, à Rio ou ailleurs, les éditions précédentes n'ont pas suscité les mêmes enjeux d'intelligence économique et de politique industrielle. Nous devrons être capables de mettre des solutions innovantes au service de tous ceux qui prendront part aux JO de Paris.

Mme Brigitte Kuster. Vous avez mentionné à plusieurs reprises la sécurité privée. À l'occasion d'une mission flash sur la sécurité des lieux de spectacles, j'ai auditionné des syndicats d'entreprises de sécurité privée, qui sont dits dépourvus face à l'échéance olympique de 2024. Ce secteur avoue une carence de personnel et de formation. Quels

conseils pourriez-vous lui donner ? Bien que ce sujet dépasse le cadre strict de notre commission, il me semble le compléter utilement.

Nous sommes, par ailleurs, à la veille des élections européennes. Si vous aviez une liste à y conduire, quelle programmation et quelles mesures préconiseriez-vous ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Une mission de coordination nationale de la sécurité des jeux olympiques de 2024 a été mise en place au ministère de l'intérieur, présidée par le préfet Lieutaud. Elle est chargée de nouer et de nourrir un dialogue avec le comité olympique ainsi qu'avec l'ensemble des acteurs, privés et publics, qui concourront à la réussite de cet événement. Les responsabilités respectives devront être définies dans ce cadre. Déjà, nous savons gérer des enjeux similaires lors des championnats de football : sécuriser la *fan zone*, organiser la sécurité à une certaine distance de ladite zone, identifier les responsabilités du maire et de l'État… Tous ces sujets devront être traités très en amont des JO de 2024.

J'en viens à votre question inattendue, madame la députée, sur les élections européennes. J'ai eu l'occasion de participer à des travaux de recherche européens il y a quelques années. Plus récemment, sous l'impulsion du ministère de l'intérieur et du secrétariat d'État chargé du numérique, j'ai pu défendre, à l'échelon européen, la question du retrait de contenus illicites publiés en ligne.

La France présente des différences manifestes avec ses voisins au regard des enjeux de sécurité. Même sur des sujets qui nous paraissent évidents – lutte contre le terrorisme, retrait de la propagande terroriste sur Internet… – il n'est pas aisé de parvenir à un consensus immédiat. Cela demande un investissement important. Il me paraît indispensable de considérer que la sécurité est un enjeu à définir au niveau européen, ce qui n'obère en rien le champ souverain que nous devons traiter sur notre territoire. La définition du partage des missions avec les acteurs européens doit reposer sur une vision et une connaissance des questions de sécurité dans le temps long. Aussi l'Union européenne doit-elle maintenir son effort de soutien à la recherche en matière de sécurité.

Aujourd'hui, au ministère de l'intérieur, cette recherche est principalement financée par des crédits européens. C'est là une grande différence avec le monde militaire. Une agence de l'innovation de défense vient d'être créée au sein du ministère des armées, dotée d'un budget de 1 milliard d'euros à l'horizon de 2022. Pour sa part, le ministère de l'intérieur répartit quelques crédits de recherche entre différents services, dans des proportions infiniment moindres. L'essentiel des projets ou des participations à des programmes de recherche relève de crédits sollicités auprès Bruxelles, le plus souvent avec d'autres partenaires européens. Cet effort communautaire doit être préservé et renforcé. Les États membres doivent au moins s'accorder sur les grandes priorités communes qu'ils jugent essentielles à une politique de sécurité européenne, sur le temps long. Les grands événements entrent d'ailleurs dans ce cadre, dans la mesure où ils sont organisés successivement par différents pays. Certes, des experts échangent déjà sur les questions de sécurité. Au-delà, ces enjeux pourraient se décliner dans une approche politique et une démarche stratégique de long terme.

M. Christophe Naegelen, rapporteur. Percevez-vous une différence notable d'équipement entre les commissariats des villes et des territoires ruraux ? Si oui, quel délai serait nécessaire pour effectuer un rattrapage ?

Pour ce qui est des programmes et logiciels communs entre la gendarmerie et la police, le fichier TAJ s'avère une vraie réussite. En revanche, le programme Neo a fait l'objet d'une déclinaison pour la police, NeoPol, et d'une autre pour la gendarmerie, NeoGend. D'autres logiciels restent spécifiques à l'une des forces. Ne serait-il pas souhaitable de centraliser et d'unifier ces outils ?

Enfin, les derniers marchés de défense ont souvent été remportés par des entreprises étrangères. Y a-t-il selon vous un risque à ce que des matériaux et des équipements relevant de la sécurité intérieure soient fabriqués dans des pays étrangers ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Je ne suis pas convaincu qu'il existe des différences considérables entre l'équipement des commissariats des villes et des zones rurales. Les systèmes d'information sont désormais unifiés. À mon arrivée à la préfecture de police, l'une de mes principales missions fut de mettre à niveau les systèmes d'information et de les aligner sur ceux de l'État. Aujourd'hui, les modalités d'accès à l'information sont homogènes. En revanche, il existe certainement des disparités en matière de parc automobile, liées aux usages. Pour m'en être occupé à Paris, je sais combien ce volet est complexe et mérite une surveillance scrupuleuse. L'usure des véhicules diffère selon qu'ils sont utilisés par les mêmes conducteurs, d'une petite unité ou par la multitude d'agents d'un grand centre de police. Les taux d'immobilisation et de disponibilité des voitures varient de surcroît selon les environnements. Pour autant, les équipements sont globalement assez proches. Je vous invite à le vérifier auprès des services en charge de ces questions.

Quant au développement de logiciels parallèles pour la police et la gendarmerie, il relève de la gouvernance et résulte de choix des directeurs généraux. Je ne saurais me prononcer sur ces arbitrages, qui sont certainement justifiés.

M. Christophe Naegelen, rapporteur. À la lumière de votre expérience, est-il justifié d'utiliser des logiciels différenciés, ou serait-il préférable d'instaurer des programmes communs ?

M. Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Sur des périmètres fonctionnels, recouvrant des missions et des métiers globalement semblables, tout doit être fait pour unifier les solutions entre les forces. Notez toutefois que des dénominations différentes peuvent cacher des similitudes assez fortes entre les outils. Ainsi, je ne pense pas que NeoPol et NeoGend soient fondamentalement différents. En revanche, les applications qui leur sont greffées peuvent engendrer des disparités. Il reste à savoir si celles-ci sont justifiées : dresse-t-on différemment un procès-verbal d'accident en zone de gendarmerie et en zone de police, par exemple ? Ces considérations méritent d'être objectivées et analysées. Toutefois, la racine même de ces outils repose sur un socle commun, administré par le service des technologies et des systèmes d'information de la sécurité intérieure. Il me semble qu'une convergence grandissante des outils est souhaitable. Idéalement, la plateforme d'appels d'urgence unifiée, le 112, devrait être supportée par un seul système d'information, capable de servir les particularités de chaque service ou entité.

J'ai eu l'occasion de signer plusieurs centaines de marchés publics, notamment en tant que directeur des services techniques à la préfecture de police. Dès lors que les acheteurs entretiennent une relation étroite avec les prescripteurs, sous l'autorité des contrôleurs, le code des marchés publics offre un cadre propice à l'élaboration de solutions innovantes, sur des

sujets complexes. C’est ainsi qu’à l’issue d’un dialogue compétitif avec plusieurs industriels, nous avons pu déployer en 2008 les premiers kits de détection de drogue dans la salive, fruits de dix ans de recherche. Ces marchés publics doivent intégrer pleinement les enjeux de filière et veiller à la préservation des intérêts des entreprises françaises et européennes. À ce titre, il est salutaire que le contrôle de l’État sur les investissements étrangers dans des secteurs sensibles inclue les entreprises qui travaillent au profit des forces de l’ordre.

M. le président Jean-Michel Fauvergue. Monsieur Delville, nous vous remercions.

*

* *

Membres présents ou excusés

Commission d'enquête sur la situation, les missions et les moyens des forces de sécurité, qu'il s’agisse de la police nationale, de la gendarmerie ou de la police municipale

Réunion du mercredi 6 mars 2019 à 16 h 15

Présents. - M. Xavier Batut, Mme Aude Bono-Vandorme, M. Jean-Claude Bouchet, M. Rémi Delatte, M. Jean-Michel Fauvergue, M. Jean-Marie Fiévet, Mme Agnès Firmin Le Bodo, Mme Marietta Karamanli, Mme Brigitte Kuster, M. Jean-Michel Mis, M. Bruno Questel, M. Jean-Louis Thiériot, Mme Nicole Trisse, Mme Laurence Vanceunebrock-Mialon

Excusés. - M. Olivier Gaillard, Mme Josy Poueyto