ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Mardi
6 avril 2021
Séance de 17 heures 30

Compte rendu n° 46

SESSION ORDINAIRE DE **2020-2021**

Compte rendu

Commission de la défense nationale et des forces armées

— Audition, à huis clos, de M. le général de corps d'armées Éric Bucquet, directeur du renseignement et de la sécurité de la défense au Ministère des Armées.

Présidence de Mme Françoise Dumas, *présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures trente.

Mme la présidente Françoise Dumas. Je suis très heureuse d'accueillir le général de corps d'armée Éric Bucquet, qui est à la tête de la direction du renseignement et de la sécurité de la défense (DRSD) depuis le mois de septembre 2018. Son audition à huis clos est l'avant-dernière de notre cycle consacré au renseignement, que nous conclurons en mai par l'audition de Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Nous aurons très prochainement l'occasion de tirer profit de nos travaux pour ce qui concerne le futur projet de loi relatif au renseignement, qui devrait être présenté en conseil des ministres à la fin du mois et examiné à l'Assemblée nationale au début du mois de juin.

La DRSD est sans doute le moins connu de nos services de renseignement, même si elle appartient au premier cercle. Elle agit dans le cadre particulier de la contre-ingérence. Sa mission principale est de renseigner les autorités sur les vulnérabilités de nos activités de défense, ainsi que sur les menaces internes et externes qui pèsent sur elles, qu'il s'agisse du personnel, du matériel, de l'information, des emprises ou des industries de souveraineté, et de contribuer aux mesures de protection pour y faire face.

Dans un contexte où les menaces hybrides prennent de plus en plus d'importance, chacun conçoit, général, que votre service est appelé à jouer un rôle toujours plus essentiel. Vous nous préciserez la place qu'occupe la DRSD au sein de la sphère du renseignement, son périmètre d'action et, si possible, ses modes d'intervention. Vous êtes particulièrement bien placé pour présenter cette synthèse, ayant été, de 2012 à 2018, directeur des opérations de la direction générale pour la sécurité extérieure (DGSE). Vous avez donc acquis une vue transversale, offensive et défensive, du monde du renseignement, ce qui est un atout déterminant dans les fonctions que vous occupez aujourd'hui.

Nous attendons aussi de vous que vous fassiez le point sur les grands défis que vous devez relever, rassemblés sous l'acronyme TESSCO : terrorisme, sabotage, subversion et crime organisé. Vous nous direz également si nous sommes bien préparés pour faire face de façon efficace aux cybermenaces, qui semblent se multiplier de nos jours, et si les militaires sont désormais bien sensibilisés aux risques de profilage numérique liés à l'usage des réseaux sociaux et des applications de sport, telles que Strava, qui a récemment défrayé la chronique. S'agissant de l'implantation, en Alsace, d'une usine Huawei à proximité de plusieurs sites sensibles de l'armée de Terre, quelle appréciation portez-vous sur la gestion du risque d'espionnage induit ?

Nous sommes également particulièrement préoccupés par le risque d'ingérence économique au sein de la base industrielle et technologique de défense (BITD). Les travaux de notre commission ont montré qu'il résulte de la crise économique provoquée par la crise sanitaire une vulnérabilité accrue de certaines entreprises, notamment des PME ayant développé des savoir-faire de pointe. Pouvez-vous nous donner votre sentiment sur cette fragilité ? Existe-t-il une menace sur la chaîne d'approvisionnement et, partant, sur notre autonomie et notre souveraineté ?

La DRSD a également pour mission de veiller au respect de l'intégrité du secret-défense. Vous nous rappellerez l'importance que celui-ci revêt et les principes qu'il convient,

de votre point de vue, de mettre en avant à l'heure où nous nous apprêtons à rénover l'articulation entre la protection du secret de la défense nationale et le libre accès aux archives datées de plus de cinquante ans, conformément aux annonces faites par le Président de la République le 9 mars dernier.

Enfin, puisque nous sommes appelés à nous prononcer sur les procédures et les budgets qui sont les vôtres, vous nous direz si les moyens dont vous disposez vous semblent suffisants et si vous souhaitez appeler notre attention sur certains points de vigilance, notamment dans le cadre de l'application de la loi du 19 mars 2015 relative au renseignement, et de l'évolution de la jurisprudence européenne relative à la collecte et à la conservation des données.

Général Éric Bucquet. Vous en savez déjà beaucoup sur la DRSD. Service de renseignement du ministre des armées, elle assure la sécurité du personnel, des informations, des matériels, des installations sensibles et des systèmes d'information. Son champ d'action est donc très vaste. Sa mission est la contre-ingérence. Elle consiste à déceler, identifier, caractériser et contribuer à entraver toute menace pesant sur la sphère de défense élargie. De telles menaces peuvent provenir d'un service de renseignement ennemi – nous en connaissons plusieurs –, d'organisations, d'agents ou d'individus, et relever du terrorisme, de l'espionnage, du sabotage, de la subversion ou du crime organisé – le périmètre de menaces, lui aussi, est large.

En tant que service de renseignement, notre rôle est de donner par anticipation des informations aux autorités. Chaque jour, une synthèse de la production des services de renseignement est adressée au Président de la République et irrigue l'ensemble des autorités politiques.

Notre champ d'investigation couvre deux domaines : la contre-ingérence des forces sur le périmètre du ministère des armées, soit près de 270 000 personnels, civils et militaires ; la contre-ingérence économique, qui vise à protéger notre BITD et les établissements de recherche associés, et plus généralement tout ce qui relève de la protection du secret de la défense nationale en matière de potentiel scientifique et technique de la nation (PSTN). Dans ces deux domaines, nous utilisons nos savoir-faire en matière de protection pour déterminer les vulnérabilités, et nos capacités de renseignement pour caractériser la menace. La synthèse de ces deux démarches nous permet de déterminer comment un ennemi pourrait nous attaquer. Sur la base de ce recoupement, nous produisons une évaluation du risque et identifions les mesures à prendre pour l'entraver.

Compte tenu de l'actualité, notre rôle est plus que jamais fondamental. Le niveau de menace n'a jamais été si élevé, et la crise provoquée par la pandémie de covid-19 l'a encore renforcé. Nos compétiteurs, qui peuvent être des États ou des organisations, voire des individus, sont multiples. Ils peuvent utiliser des moyens légaux, tels que la *compliance* de nos amis Américains, ou recourir à la violence, tant physique que virtuelle. Au demeurant, la cyberdéfense est pleinement intégrée à nos actions de contre-ingérence.

La DRSD emploie environ 1 500 agents. Elle dispose d'un budget de 150 millions d'euros, dépenses de personnel comprises. Elle exerce sa mission de contre-ingérence partout où se trouvent des militaires français et des entreprises liées au secteur de la défense. Nous sommes implantés sur le territoire national, dont nous assurons le maillage par le biais d'une

cinquantaine d'implantations, outre-mer et à l'étranger – nous couvrons les contingents basés hors de la métropole et les forces déployées en opérations extérieures (OPEX) –, où nous disposons d'une vingtaine d'implantations, soit au total environ soixante-dix postes et détachements dans nos frontières et à l'étranger, ce qui est assez spécifique pour un service de renseignement.

Au quotidien, la DRSD travaille en étroite collaboration avec les autres services de renseignement, qu'ils appartiennent au premier cercle ou au second, ainsi qu'avec les structures institutionnelles que sont l'agence nationale de la sécurité des systèmes d'information (ANSSI), le service de l'information stratégique et à la sécurité économiques (SISSE) et les préfectures. En matière de maillage territorial et de collaboration, nous avons réalisé les progrès les plus significatifs. Notre service prend une part active aux initiatives de mutualisation et de partage de l'information et des moyens techniques, même si nous maîtrisons nos propres techniques, autorisées par la loi du 24 juillet 2015 relative au renseignement. Nous avons constitué un réseau d'officiers de liaison. Nous sommes parfaitement intégrés dans la communauté du renseignement et de la lutte cyber.

Face à une menace toujours plus grande, plus forte, plus agile et plus technique, la DRSD s'est lancée, il y a trois ans, dans un vaste mouvement de transformation technologique, accompagné d'une remontée en puissance en matière de ressources humaines. Nous menons une véritable révolution au sein de la DRSD, à travers trente-quatre chantiers de modernisation. Les objectifs sont clairs : dynamiser et accélérer la collecte du renseignement, véritable ADN du service, tout en consolidant notre expertise dans nos missions de protection.

Parmi nos domaines de lutte prioritaire, le terrorisme occupe la première place. Sa montée en puissance date de 2015. Depuis ma prise de fonction, je ne cesse d'affirmer à mes équipes que la lutte antiterroriste demeure notre priorité numéro un ; notre détermination à ce sujet est sans faille. La crise sanitaire représente également un risque considérable pour notre BITD. Les entreprises doivent affronter non seulement une tourmente économique, avec la perte d'affaires, mais aussi des concurrents ayant en partie retrouvé une pleine capacité opérationnelle. Le niveau de vulnérabilité de nos entreprises est immense, et le besoin de protection de nos intérêts stratégiques n'a jamais été aussi avéré.

Ces deux crises majeures, terrorisme et crise économique, exigent une pleine mobilisation des deux piliers de la DRSD que sont sa capacité de protection et sa capacité de renseignement – les résultats obtenus sont tangibles. Elles exigent également la poursuite de la transformation de la DRSD, notamment pour adapter ses processus aux nouvelles technologies. Je dois avouer que nous avons plus que jamais besoin de moyens financiers et humains pour mener à bien cette transformation humaine, technologique et immobilière. J'aborderai ce sujet après avoir fait le point sur la menace terroriste et les ingérences économiques, qui constituent des priorités pour la DRSD, dans l'environnement cyber comme dans l'environnement physique.

S'agissant de la lutte anti-terroriste, au sein de la sphère de défense, la menace est réelle. Bien entendu, nous sommes une cible de choix. Nos personnels portent le plus souvent des armes ; certains, dans le cadre des opérations « Sentinelle » et « Résilience », patrouillent dans les rues, parmi les civils auxquels des terroristes pourraient s'attaquer.

Pour contenir la menace, nous procédons tout d'abord à de nombreuses enquêtes administratives. En 2020, nous en avons mené 311 000. Nous passons au crible nos propres agents, ainsi que les personnels militaires et civils du ministère des armées et les personnels des entreprises contractantes ayant accès à des informations classifiées. Sur ce sujet, nous avons mené une véritable révolution pour aller de plus en plus vite. Avant la crise économique, ces entreprises étaient en plein boom. L'adoption de la loi de programmation militaire (LPM) 2019-2025 avait favorisé une reprise des activités industrielles et de recherche, concomitante d'un fort renouvellement des personnels au sein des entreprises de défense en raison de leur pyramide des âges. Nous avons donc accéléré nos processus afin de résorber les enquêtes non traitées, que nous appelions « dette ».

Un tel résultat a exigé de mobiliser des ressources humaines supplémentaires et de moderniser nos systèmes d'information, afin de les rendre plus performants, plus rapides et plus ergonomiques. Je reviendrai sur ce point lorsque j'aborderai la transformation de la DRSD.

Ces enquêtes administratives constituent un premier rempart contre la menace terroriste. Elles permettent d'empêcher qu'un individu radicalisé ou présentant un risque pour la défense ne soit recruté par une entreprise de la BITD ou ne pénètre dans l'une de nos emprises. C'est en grande partie grâce à elles que la menace terroriste est contenue.

Nous complétons ce travail d'enquête administrative par nos activités de renseignement, qui reposent au premier chef sur une coopération entre les services, dans laquelle la DRSD a pris toute sa place, notamment au sein d'organisations de création récente, et de cellule de coopération dédiée. À présent, l'information circule vite et bien entre les services de renseignement, ce qui nous permet d'accroître notre efficacité.

Notre activité de renseignement au sein du ministère des armées repose également sur des actions de sensibilisation contre les radicalisations, et sur un réseau de référents. Ce système, associé à une culture du compte rendu solidement installée au sein des armées, est robuste. Il permet d'écarter tout profil susceptible de radicalisation.

Plus généralement, l'armée offre un cadre peu perméable à la radicalisation. Tout soldat bénéficie d'un commandement de proximité, qui repère vite d'éventuelles difficultés. Les armées fournissent également un référentiel de valeurs et instituent un esprit de corps, lesquels forment un environnement peu propice à la radicalisation.

Toutefois, nous devons nous montrer humbles et vigilants, et perfectionner nos dispositifs de contrôle, selon une démarche que je détaillerai ultérieurement.

La DRSD porte également une attention toute particulière au risque que les mouvances de l'ultradroite et de l'ultragauche font peser sur le ministère des armées. Au sein de sa direction centrale, des effectifs leur sont spécifiquement dédiés. Face à ce risque, l'objectif est d'identifier et, le cas échéant, d'entraver les mouvements visant à nuire à la défense nationale, en portant atteinte à l'image des armées ou en tentant de recruter des militaires. Il s'agit également de détecter les personnels adhérant à une idéologie incompatible avec les valeurs de la République française, au sujet desquels Mme la ministre des armées a été très claire dans un discours prononcé il y a quelques semaines.

Quant aux actions d'ingérence économique, elles atteignent des niveaux d'intensité inédits. La crise sanitaire place notre BITD dans une situation de faiblesse tout aussi inédite, fragilisant la situation financière des entreprises et les rendant plus vulnérables à la prédation capitalistique. Le tissu des petits fournisseurs est également menacé, dès lors que les carnets de commandes s'amenuisent. Le recours massif au télétravail démultiplie les capacités d'action des cybercriminels. Les risques sont donc considérables, d'autant que nos concurrents ont retrouvé pour une large part leur pleine capacité opérationnelle. J'ai demandé à mes services de rester pleinement mobilisés et de garder le contact, même pendant le confinement, avec nos industriels. Cela n'a pas été sans difficulté, la crise sanitaire empêchant de dialoguer selon nos habitudes. Nous avons dû adapter nos dispositifs. Par-delà le rapport direct avec l'entreprise et le poste compétent, nous avons régulièrement transmis une lettre d'information aux chefs d'entreprise de notre périmètre.

Fort de son maillage territorial national, la DRSD est pleinement impliquée, au quotidien, auprès des acteurs de la BITD, notamment dans le domaine cyber. De l'entreprise du CAC40 à la petite start-up, le service agit à plusieurs niveaux : tout d'abord par les sensibilisations qu'il effectue, des collaborateurs aux membres des comités exécutifs (comex) ; ensuite par ses conseils techniques, l'émission d'avis et le contrôle de l'application des règles de sécurité.

Par ailleurs, si une entreprise connaît une attaque cyber, la DRSD est en mesure de conduire des investigations à son profit pour caractériser l'origine et la nature de l'attaque et de l'assister par son conseil. L'idée est de protéger l'ensemble de la BITD. L'intégration du service au sein du groupement d'intérêt public Action contre la cyber malveillance (GIP ACYMA) en février dernier, en qualité de représentant permanent du ministère des armées, aux côtés d'importants acteurs étatiques tels que l'ANSSI, consacre son action et son professionnalisme dans ce domaine hautement technologique. La création de cette entité, en mars 2017, dans le cadre de la stratégie nationale pour la sécurité du numérique, concrétisait la volonté gouvernementale de répondre aux besoins des particuliers, des entreprises et des collectivités territoriales, hors opérateurs d'importance vitale et opérateurs de services essentiels.

Convaincu que la collaboration entre les services démultiplie leur efficacité, en particulier sur le terrain, je me félicite du travail que nous réalisons avec la DGSI. En matière de sécurité économique, la DRSD et la DGSI sont services menants ; les autres services sont des services concourants. La délimitation de nos compétences et de nos coopérations a été précisée cette année. À présent, l'échange de renseignements entre nos deux services est d'excellente qualité.

Les résultats de cette mobilisation sont à la hauteur de la menace. En 2020, nous avons rédigé plusieurs centaines de notes de renseignement dans le domaine de la contre-ingérence économique, soit une augmentation de 36 % par rapport à 2019.

Toutefois, si le renseignement élaboré est abondant, nous devons nous mobiliser davantage pour que des mesures de protection et d'entrave soient prises en temps et en heure, s'agissant notamment des secteurs particulièrement ciblés que sont le nucléaire, la construction navale et le spatial. Dans ce dernier domaine, l'action de nos équipes en Guyane est importante. Elles participent directement à la sécurité de l'agenda spatial, très chargé pour les prochaines années.

Dans le domaine naval, le contrat *Australian future submarine program* (AFSP), remporté par Naval Group pour un montant initial de 34 milliards d'euros, porté à 50 milliards avec le maintien en condition opérationnelle (MCO), mobilise également les moyens du service. Nous menons régulièrement des inspections physiques et cyber au sein du groupe, au siège social et dans ses divers établissements, ainsi qu'auprès de ses principaux fournisseurs. Nous nous assurons également de la sensibilisation des acteurs privés et publics à la nécessaire protection dans le cadre de ce contrat stratégique pour nos deux pays.

Par ailleurs, nous apportons une contribution importante à la protection du potentiel scientifique et technologique de la Nation (PSTN) en menant des missions d'inspection des sites militaires et industriels. Nous sommes parvenus à rétablir un taux d'inspection satisfaisant, notamment en augmentant le nombre d'inspecteurs et en diversifiant les viviers de recrutement. En 2021, nous devrions parvenir à une performance similaire, sauf à ce que le rétablissement du confinement ne nous empêche d'atteindre cet objectif. En tout état de cause, nous mettons tout en œuvre pour garantir l'inspection de tous les points d'importance vitale (PIV).

Avant de conclure, j'aimerais évoquer deux autres axes d'efforts dans le domaine du renseignement.

En matière de lutte contre l'espionnage, la menace demeure à un niveau très élevé, dont j'estime qu'il est en progression. Les événements régulièrement relatés dans la presse permettent au grand public de percevoir combien les services de renseignement adverses conservent une activité agressive. Nous utilisons les moyens traditionnels, ainsi que les possibilités d'attaques ciblées et sophistiquées offertes par le champ du cyber.

Dans ce domaine, nous sommes restés très actifs cette année. Nous avons notamment créé une cellule opérationnelle de réaction aux incidents cyber.

En tant que service de renseignement, la DRSD intervient dans un périmètre de compétence qui nous est propre avec des moyens variés, au premier rang desquels le recours possible à toutes les techniques de renseignement autorisées par la loi du 24 juillet 2015. Je milite aussi pour un renforcement de la coopération entre les services dans le domaine cyber, notamment en vue d'un échange plus systématique des marqueurs répertoriés.

Comme vous pouvez le constater, l'année 2020 et l'année en cours sont, pour la DRSD comme pour la société française dans son ensemble, particulièrement complexes. À aucun moment nous n'avons baissé la garde, bien au contraire. Nous avons connu un niveau d'activité inédit. Ma conviction que la DRSD doit accélérer sa transformation en gardant à l'esprit ses deux priorités – le terrorisme et la contre-ingérence économique – s'en trouve renforcée.

Cette transformation s'est poursuivie en 2020 et demande à être consolidée par l'apport de moyens humains et financiers. Pour faire face aux menaces et retrouver des marges de manœuvre, la DRSD se transforme en service de renseignement dit « de temps de crise durable » à travers une nouvelle organisation, une modernisation technologique et immobilière, une remontée en puissance des ressources humaines. Dans tous ces domaines, les avancées sont importantes.

Ainsi la nouvelle organisation est-elle désormais pleinement opérationnelle : un état-major coordonne l'action des sous-directions, dont la nouvelle sous-direction technique. Une direction zonale, hors métropole, a également été créée et dynamise l'action de la centaine d'agents répartie dans le monde. Je souligne que les capacités que nous offrons outre-mer et en OPEX sont de plus en plus sollicitées par nos autorités.

Sur un plan technique, ma priorité demeure la création d'un nouveau système de recueil et d'exploitation du renseignement, afin de franchir une nouvelle étape en matière de traitement de données massives – *big data* – et de donner des outils à nos agents pour enrichir et accélérer leurs analyses. Ce projet est désormais en phase de réalisation avec un grand systémier. Nous avons choisi une modalité de développement innovante en retenant la méthode agile, dans le cadre d'un travail collectif entre nos ingénieurs respectifs. Chaque année, une partie du système devient opérationnelle et, à la fin de 2021, nous disposerons d'une solution complète et souveraine, ce qui sera une première, pour un coût plus que compétitif.

Le Service a également souhaité améliorer ses processus d'enquête administrative, ce qui était indispensable dans un contexte de menaces terroristes de plus en plus importantes. Ainsi deux projets reposant sur l'intelligence artificielle et le *machine learning* sont-ils en cours de finalisation. Il s'agit de mener les enquêtes plus rapidement et de manière plus approfondie.

En matière d'enquêtes administratives, plusieurs rapports d'inspection ont jugé les processus de la DRSD comme étant les plus robustes. Avec l'achèvement de ces deux nouveaux projets, nous franchirons une nouvelle étape et nous en partagerons les fruits avec les autres services de la communauté du renseignement. Nous suivons également avec intérêt d'autres projets portés par des services partenaires. En revanche, nous ne travaillons pas avec la Fabrique Défense, car nous n'avons pas de besoins particuliers et le nombre de ressources humaines dont nous disposons est limité.

Notre modernisation technologique s'accompagne d'une restructuration immobilière, qui concerne essentiellement la direction centrale et vise trois objectifs : accueillir les nouveaux personnels, offrir des fonctionnalités supplémentaires – salles d'entretien, amphithéâtre pour les formations – et accélérer le cycle du renseignement en regroupant tous les services, opérationnels et experts, et en décloisonnant les espaces. Le programme du futur bâtiment est achevé et le contrat de réalisation sera notifié prochainement, pour une livraison à la fin de 2023. Nous restons évidemment très vigilants pour que la dotation budgétaire correspondante soit bien inscrite dans la programmation de la gestion 2021 du programme 144.

Enfin, les ressources humaines (RH) remontent en puissance. Des moyens supplémentaires ont été ainsi attribués à la DRSD, même s'ils ont été évalués au plus juste et que notre charge de travail n'a cessé de croître.

Si des droits à recrutement nous ont été ouverts, encore la DRSD devait-elle gagner la bataille des talents pour recruter les spécialistes dont elle a besoin. Je suis très heureux que, malgré la crise sanitaire, nous ayons pu atteindre nos objectifs « RH » en 2020. Au 31 décembre 2020, le service a ainsi atteint 98 % de sa cible. Le dépassement du cap des 1 500 est symbolique, car il correspond aux effectifs du début des années 2000, alors que nous

étions 1 000 en 2013. C'est le début de la remontée en puissance RH et de la croissance réelle des effectifs.

Pour atteindre une telle performance, absolument inédite, nous avons diversifié nos viviers de recrutements en faisant plus largement appel aux personnels civils. À ce jour, plus de 30 % de nos agents sont civils et apportent à la DRSD les compétences qui lui manquaient : linguistes, *data scientists*, cyber-ingénieurs, etc.

La DRSD a changé de visage : elle s'est rajeunie et le niveau moyen de compétences a augmenté, à travers notamment le recrutement de personnels de catégorie A. Nous avons également créé de nouveaux métiers que nous avons pu ouvrir aux agents civils. Depuis deux ans, les agents de contre-ingérence économique, les « ACIÉ », sont recrutés après un Master 2 et sont déployés au sein de notre maillage territorial ; avec une efficacité au-delà de nos attentes, ils complètent l'action de nos traditionnels inspecteurs de sécurité de la défense, maillons essentiels de la collecte de renseignement d'origine humaine qui demeurent indispensables. Les effectifs sont désormais au complet alors que, depuis de nombreuses années, nous souffrions d'un déficit important dans cette spécialité.

Pour parvenir à recruter de nombreux agents et que la « greffe prenne » sur une courte période, nous avons appliqué une stratégie de fidélisation sur les moyen et long termes. Ainsi, nous avons organisé de nouveaux parcours professionnels en trois étapes – junior, senior, expert – afin de donner des perspectives de carrière à tous nos agents de renseignement et d'offrir un cadre pour les accompagner dans leur formation et le maintien de leurs compétences. Ces parcours prévoient des mobilités interservices permettant de développer des réseaux, d'accroître ses compétences et, tout simplement, de mieux se connaître : c'est là, en effet, l'une des clés pour travailler en étroite collaboration et fluidifier nos échanges. Ce projet, ambitieux, est également incitatif, car il s'accompagne d'une réforme du régime indemnitaire de la DRSD visant à l'articuler avec les trois étapes du nouveau parcours professionnel que je viens de mentionner.

Le constat RH est donc globalement positif. J'ai, de surcroît, le sentiment que mes agents sont heureux : même dans les épreuves, ils gardent un enthousiasme que j'ai rarement rencontré. Cela se traduit par une diminution du *turn-over* qui, de 14 % en 2014, a chuté à 10 % en 2020. Des inquiétudes, néanmoins, demeurent, en particulier s'agissant des sous-officiers expérimentés : les armées peinent toujours à nous fournir cette ressource et nous arrivons aux limites de la civilianisation. Le service doit, en effet, préserver son socle opérationnel, c'est-à-dire sa capacité à réaliser des opérations dans la durée et à déployer en OPEX un certain nombre de militaires.

Par ailleurs, le service doit faire face à l'augmentation des postes d'officiers de liaison auprès de structures partenaires induite par le renforcement constant de la coopération opérationnelle : à ce jour, vingt-trois personnels sont détachés dans différentes instances. Cette augmentation correspond à un besoin RH inédit, lequel doit être également pris en compte.

Notre feuille de route est donc dense, alors que le contexte sécuritaire et géopolitique n'a jamais été aussi tendu. Le budget qui nous est attribué dans la loi de finances est taillé au plus juste et tout nouveau projet exige de trouver un financement ad hoc.

Après une année budgétaire record, en 2020, pour financer les deux premières tranches de notre nouveau système d'information, la DRSD atteint en 2021 un premier plateau d'environ 20 millions en autorisation d'engagement, hors crédits de personnels. Pour une très grande part, cette dotation est consacrée aux dépenses permettant de recueillir le renseignement.

En effet, nous avons choisi, dans la LPM, de geler nos dépenses de fonctionnement pour privilégier l'activité opérationnelle et l'investissement. Un tel choix est particulièrement difficile alors que nos effectifs augmentent : nous avons dû rationaliser notre fonctionnement en passant en revue tous les postes de dépense. Je crois que nous sommes arrivés au bout de cette logique qui nous a toutefois offert des marges de manœuvre pour nous moderniser. Nous continuerons en ce sens en 2021. Ainsi, nous achèverons les projets optimisant et accélérant nos enquêtes administratives. La dotation 2021 financera également les opérations nécessaires pour assurer la transition imposée par la nouvelle instruction générale interministérielle IGI 1300 fixant les dispositions relatives à la protection du secret de la défense nationale.

Le service poursuit donc sa transformation en optimisant au maximum l'emploi des ressources. Cependant, compte tenu de la croissance régulière de ses missions et de l'évolution constante de la menace sur l'ensemble du spectre TESSCO, une nouvelle impulsion budgétaire et RH sera, de mon point de vue, nécessaire à moyen terme pour parachever cette transformation et donner à la DRSD sa pleine puissance.

Un mot, pour conclure, sur l'adéquation des besoins du service au cadre légal offert par la loi relative au renseignement de 2015. Alors que le besoin de protection n'a jamais été aussi fort, la préservation des capacités d'action des services me paraît nécessaire. Je plaide en faveur d'une stabilité du dispositif actuel qui a trouvé son équilibre. Nous souhaitons donc quelques évolutions de bon sens mais pas de révolution à l'occasion du prochain réexamen de cette loi.

Je reste également très vigilant quant à toute tentation de limiter nos capacités, ce qui serait malvenu alors que les diverses menaces pesant sur la France n'ont jamais été aussi nombreuses. Ainsi la jurisprudence Tele2 « Quadrature du Net », dans sa version française, est très inquiétante et paraît en totale contradiction avec les attributions de l'Union européenne. J'espère que, collectivement, nous trouverons une solution pour permettre aux services de renseignement de travailler efficacement à la sécurité des Français.

Mme Florence Morlighem. La DRSD est un maillon essentiel de l'outil de renseignement français dans la contre-ingérence de défense au sein des forces elles-mêmes et des 4 000 entreprises stratégiques pour l'outil militaire national.

Un enjeu me préoccupe particulièrement : celui des conséquences de la jurisprudence européenne Tele2, imposant à chaque législateur une conservation ciblée, sous condition, des données. La Cour de justice de l'Union européenne a confirmé cet arrêt le 6 octobre 2020 en s'opposant à la transmission ou à la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation des citoyens européens à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale. Des précisions ont été apportées le 2 mars 2021 : l'accès à des fins pénales à un ensemble de données de communications électroniques relatives au trafic ou à la localisation permettant de tirer des

conclusions précises sur la vie privée n'est autorisé que pour lutter contre la criminalité grave ou prévenir des menaces graves contre la sécurité publique.

L'arrêt Tele2 peut donc avoir des conséquences très importantes pour la communauté du renseignement. Le procureur général près la Cour de cassation et ancien procureur de Paris, M. François Molins, qui a dû gérer l'essentiel de la vague des attentats terroristes de 2015 à 2018, juge la décision Tele2 matériellement irréaliste. La conservation des données peut être primordiale pour les services de renseignement afin d'avoir un recul sur les personnes identifiées : un individu dont les actions sont remarquées par les services de renseignement peut en effet disparaître des radars et reprendre quelques années plus tard ses néfastes activités. Quelles sont, selon vous, les conséquences de la jurisprudence Tele2 pour la DRSD ? Ne pas conserver de traces des actions des individus concernés ne fait-il pas courir un risque très important à notre pays ?

La DRSD doit évidemment poursuivre ses activités pendant la crise sanitaire sans précédent que nous traversons afin notamment d'assurer la protection des forces engagées en OPEX ou dans l'opération Résilience. Les menaces auxquelles nous sommes confrontés peuvent encore s'accroître en raison de la covid 19. Pourriez-vous faire un point sur les conséquences de cette épidémie sur les activités de votre service ?

M. Jean-Louis Thiériot. Nous sommes évidemment très conscients de l'apport considérable de la DRSD. J'ai eu l'occasion de travailler avec la direction de la protection et de la sécurité de la défense (DPSD) – le nom que portait votre service lorsque j'étais officier de réserve dans la marine – et j'ai pu en mesurer toute son importance.

Je viens de réaliser deux missions flash, l'une avec ma collègue Françoise Ballet-Blu sur le financement de la BITD, et l'autre sur le rôle de l'industrie de défense dans la politique de relance. Vous avez évoqué la *compliance*. Des industriels de la défense ou des services qui y contribuent nous ont alertés sur les *compliance officers* qui, dira-t-on, sont informés de bien des choses, ce qui peut entraîner des risques de fuites vers des puissances étrangères, notamment à travers l'utilisation des logiciels KYC, « *Know your customer* », en particulier, en matière de *mapping* des relations des entreprises de la BITD. Quelle est votre analyse à ce propos ?

Avez-vous noté une intensification de la guerre réputationnelle et des opérations d'ingérence menées par certaines ONG ?

Enfin, en l'état du droit, qu'en est-il des possibilités de judiciarisation de certains faits ? Des améliorations vous semblent-elles nécessaires ?

Mme Sabine Thillaye. Nous sommes tous préoccupés par la cybersécurité, qui ne doit supporter aucun maillon faible. Le ministère des Armées a annoncé qu'un milliard d'euros y sera consacré, mais qu'en est-il plus précisément de l'accompagnement des collectivités territoriales ? Avec quels acteurs territoriaux échangez-vous directement ? Si tel n'est pas le cas, une collaboration étroite entre vos services et les élus locaux n'est-elle pas souhaitable, notamment en matière de formation à la cybersécurité ?

M. David Habib. Pourriez-vous préciser en quoi la loi relative au renseignement, que nous sommes quelques-uns à avoir votée, pourrait-elle être améliorée ?

Que pouvez-vous dire de la menace nucléaire iranienne ?

Les personnels militaires, avez-vous dit, sont peu perméables à la radicalisation et c'est le discours que les responsables de la préfecture de police de Paris ont longtemps tenu, jusqu'à l'attentat de 2019. J'espère que ce « laisser-faire » n'est plus de mise.

Enfin, avez-vous noté au sein de vos effectifs des difficultés liées aux différences de cultures – générationnelles, entre civils et militaires, entre personnels de niveaux de formation différents ?

M. Jean-Charles Larsonneur. Récemment, Mediapart a dévoilé une liste de cinquante néonazis au sein de l'armée française. Il ne s'agit évidemment pas d'une filière, les armées recrutant chaque année 26 000 militaires, mais d'une goutte d'eau parmi les 210 000 militaires qui composent nos forces. De surcroît, une bonne dizaine a déjà quitté les armées. Il n'en reste pas moins que nos concitoyens attendent légitimement des réponses. Pourriez-vous nous éclairer sur la lutte contre la radicalisation au sein de nos forces armées et sur la manière dont vous criblez ces individus ?

Par ailleurs, un officier de la marine italienne a été récemment arrêté en flagrant délit d'espionnage au profit de la Russie. En 2020, un officier français en poste à Naples, à l'OTAN, avait également livré des informations au GRU, le service de renseignement militaire de la Russie, lequel semble donc particulièrement actif auprès de nos officiers supérieurs. Pourriez-vous caractériser plus précisément cette menace ?

Enfin, Mme la présidente a cité des installations civiles chinoises, notamment Huawei, qui présentent des risques pour certains sites sensibles français. De la même manière, on évoque la présence d'étudiants chinois en Bretagne près de sites sensibles. Pourriez-vous préciser l'étendue et les caractéristiques de la menace chinoise ?

M. Yannick Favennec-Bécot. Lors d'un entretien que vous avez accordé à l'Association de soutien à l'armée française, le 14 avril 2020, vous avez abordé la question des jeunes retraités de l'industrie de la défense et des actifs pouvant faire l'objet de tentatives de recrutement de la part d'acteurs étrangers, notamment de la Chine. Il va sans dire que cela présente des risques importants en matière de transfert de technologies. De tels risques sont-ils fréquents ? Vos services les ont-ils quantifiés ? Quels sont les moyens employés par ces acteurs étrangers pour approcher et contacter ces Français ? Lorsque de tels rapprochements se produisent, comment vos agents agissent-ils ? Comment vos services travaillent-ils à la sensibilisation des entreprises ? Enfin, vos inspections simulent-elles régulièrement des rapprochements étrangers pour vérifier la fiabilité d'un individu ?

M. Bastien Lachaud. Concernant l'ultradroite, on a l'impression, à la lecture de l'enquête de Mediapart, qu'il a fallu cette enquête journalistique pour que des sanctions soient prises. J'imagine que ce n'est pas le cas, mais pourriez-vous nous indiquer combien de personnes radicalisées d'extrême droite vous avez criblées et combien vous en suivez ? Quelles suites sont données ?

Il y a quelques mois, la presse a fait état d'un potentiel trafic d'armes au profit de mouvances d'extrême droite, dans lequel des militaires auraient été impliqués. Pouvez-vous nous en dire plus ?

Le 3 février, les données de santé de 500 000 patients français, dont plus de 2 000 militaires et des personnels travaillant dans le renseignement, ont fuité. Quelle est l'ampleur réelle de cette fuite de données concernant nos militaires, notamment les personnels de renseignements sous couverture ? Quelles conséquences a-t-elle eues sur le fonctionnement des armées et des services ? Quelles dispositions avez-vous prises et quelles recommandations avez-vous transmises pour que cela ne se reproduise pas ? Les données de santé sont particulièrement sensibles ; elles constituent un moyen de pression sur les militaires pour les services de renseignement étrangers. Avez-vous notamment préconisé que tous les examens de santé de nos militaires et de leurs familles soient réalisés par le service de santé des armées (SSA). Comment sont sécurisées les données de santé détenues par le SSA ?

M. André Chassaigne. Dans une interview, vous avez comparé la DRSD à un Futuroscope, bien éloigné du cliché de la vieille maison poussiéreuse, en faisant notamment allusion aux habilitations de sécurité. Ce travail d'investigation, avez-vous dit, nécessite des technologies de pointe et des algorithmes complexes. Vous nous avez également expliqué qu'une telle technicité exige du personnel en nombre, mais aussi des compétences. Vous estimez que la bataille des talents a été gagnée – ou qu'elle est sur le point de l'être. Pour autant, devez-vous faire appel à des entreprises privées de prestation de services, notamment des start-up, qui viennent soutenir vos équipes d'ingénierie, car il est difficile de disposer de toutes les compétences – experts en mégadonnées ou *data scientists*, cyberlinguistes et autres développeurs informatiques spécialistes des finances ? Ou bien la coopération avec les autres acteurs institutionnels, comme l'ANSSI, la DGSE ou le COMCYBER, suffit-elle à répondre aux besoins ?

Les start-up ont beaucoup de difficultés à se protéger, et ce n'est souvent pas leur priorité, ce qui les rend d'autant plus vulnérables. Ne faudrait-il pas uniquement faire appel à de grandes entreprises privées, beaucoup plus sécurisées, comme Orange Cyberdéfense, Thales, CS GROUP, Airbus Defence and Space, etc. Quelle est la part des partenariats avec des entreprises privées et quelle est la nature de votre coopération avec les autres acteurs institutionnels ?

Mme Josy Poueyto. Vos propos éclairants nous interpellent cependant. Si nous faisons face à l'augmentation et à la récurrence de cyberattaques perpétrées directement sur notre territoire, et peut-être encore davantage durant cette période de crise sanitaire, le phénomène ne semble pas non plus étranger aux théâtres d'opérations extérieures. Ainsi la 807e compagnie de transmissions (807e CTrs), qui a pour mission de contrer les cyberattaques contre Barkhane, a-t-elle recensé une attaque informatique tous les dix jours au Sahel. Quel est le rôle de la DRSD en matière de contre-ingérence au Sahel, et plus largement là où la France dispose d'intérêts nationaux à l'étranger ?

Mme Patricia Mirallès. Vous occupez une fonction primordiale dans la protection de notre base industrielle et technologique de défense face aux regards malveillants que des puissances étrangères ou des groupes d'intérêts économiques pourraient porter sur elle. L'armée de terre a récemment lancé un Battle-Lab Terre à Satory, sous l'impulsion du ministère des armées et des différentes structures contribuant à alimenter nos armées en matériels innovants. Cette initiative permet d'accélérer les processus de développement des systèmes d'armement, mais surtout de faciliter la mise en relation entre les capacités d'innovation et de production et les besoins concrets des troupes.

Ce système est très pertinent et il ne s'agit aucunement de le remettre en cause. Cependant, l'exposition au grand jour des prototypes destinés à nos forces, ainsi que l'inclusion de très nombreux acteurs du secteur privé, augmentent considérablement les risques d'espionnage industriel et de détournement de ces innovations par des puissances concurrentes. Comment concilier le besoin de mise en relation directe des industriels avec les militaires exprimant des besoins précis et la nécessité de protéger au mieux les innovations dans un contexte accru de guerre économique ?

M. Jacques Marilossian. Je vous poserai la même question que celle soumise il y a un mois à votre homologue, le général Ferlet, directeur du renseignement militaire (DRM). Dans un article publié dans *Défense et sécurité internationale*, Roger Noël, spécialiste du renseignement, explique les difficultés des services de renseignement français à mener leurs missions de contre-terrorisme par le manque de capacité ou de volonté de la communauté du renseignement de conceptualiser les échecs et de penser contre elle-même. En conséquence, les services de renseignement subissent un manque de coordination et d'impulsion stratégique.

La DGSE serait le seul service à produire des études de ce type, avec un cercle de réflexion baptisé Interaxions. La DRSD luttant également contre le terrorisme, doit-elle réfléchir à ses éventuels échecs et les conceptualiser dans le cadre d'études stratégiques ? Si oui, comment ?

Mme Muriel Roques-Etienne. La direction du renseignement et de la sécurité de la défense est, selon les termes de l'article D. 3126-5 du code de la défense, le service dont dispose le ministre des armées pour assumer ses responsabilités notamment en matière de sécurité du matériel. Corapporteure d'une mission d'information sur les marchés publics de défense et de sécurité, je souhaiterais savoir si votre service suit des orientations particulières en termes de commande publique.

Ce service maille le territoire national et dispose de ressources humaines et matérielles importantes. À ce titre, il connaît et échange avec les entreprises de l'industrie de la défense. Votre domaine d'action étant éminemment lié à la souveraineté nationale, parvenez-vous à vous fournir en France et dans quelle proportion, alors qu'un effort sans précédent vise à relocaliser les activités industrielles stratégiques en France et que la consolidation de l'industrie de défense est un enjeu fort ? Avez-vous des difficultés à identifier des fournisseurs français et européens auxquels vous pourriez avoir recours ? Parvenez-vous à faire en sorte que plusieurs entreprises concurrentes se positionnent sur un même marché, à garantir un allotissement permettant aux plus petits acteurs de l'industrie de défense de répondre à ces marchés ?

Plus largement, les règles des marchés publics qui s'appliquent à votre service sont fixées par une directive européenne, qui prévoit des dérogations pour les activités de renseignement. Ces règles doivent-elles évoluer afin de faciliter votre fourniture en équipements ?

Mme Sereine Mauborgne. Parmi les questions urgentes et essentielles, celle des habilitations me semble primordiale. Il faut parfois trois à six mois pour habiliter les personnels de sous-traitants à entrer dans des zones militaires dans certains départements. De même, certaines PME et PMI attendent longtemps leur habilitation « secret défense » et

travaillent à l'ombre des grandes sociétés précédemment citées, comme Orange ou Atos. Elles risquent de quitter la France et de vendre à l'étranger des innovations de rupture et notre supériorité stratégique.

Mme Carole Bureau-Bonnard. Vous avez parlé de l'immense vulnérabilité des PME et PMI, notamment due à la crise économique. Pourriez-vous développer ? Cette vulnérabilité pourrait-elle engendrer de la désorganisation et perturber l'organisation de surveillance des personnels ou des entreprises concernées ?

Général Éric Bucquet. Nous avons effectivement des inquiétudes concernant la vulnérabilité de certaines PME et PMI dont les carnets de commandes sont vides ou qui n'ont pas eu les commandes qu'elles attendaient, et qui sont en outre gênées dans leur fonctionnement par les contraintes sanitaires, tout en subissant la concurrence extérieure. Les risques sont donc de plusieurs ordres : l'entreprise peut faire faillite, avec des conséquences sociales que cela implique ; elle peut être rachetée par une société étrangère. C'est pourquoi, comme la DGSI, nous restons en contact avec les entreprises pour connaître leurs difficultés, essayer de les analyser avec elles, puis remonter ces informations le plus rapidement possible vers le service de l'information stratégique et de la sécurité économique afin d'apporter, si besoin, des mesures correctrices et d'essayer de les soutenir.

À ce stade, en dépit de vulnérabilités importantes, il n'y a pas de catastrophe. Les mesures gouvernementales, complétées par le chômage partiel, constituent un bon amortisseur, toutes les entreprises le disent. Nous sommes plus inquiets pour le futur, au terme de la crise sanitaire, dans six mois. Notre crainte est double : le potentiel rachat de fleurons technologiques, entreprises françaises exceptionnelles, par des étrangers, et donc leur disparition, le savoir-faire partant à l'étranger – on l'a déjà vu par le passé ; la rupture de la chaîne de valeur de certains grands groupes, qui ne pourraient plus construire leurs systèmes d'armes, l'entreprise française habilitée et accréditée qui y participait n'étant plus disponible.

Les habilitations des PME et PMI sont une priorité, et cela dès mon arrivée en 2018 – j'avais rencontré les patrons de ces entreprises, qui n'en pouvaient plus et se plaignaient de la lenteur du sytème. Grâce à un effort considérable et la mise en place d'une *task force*, nous avons résorbé notre dette et modernisé le dispositif. Je ne reçois d'ailleurs plus de plaintes des entreprises ; le taux de réponse dans les délais, tel qu'il est décrit dans le PAP, est de 93 % et nos délais sont inférieurs aux quatre mois légaux. Ces délais sont tenus alors qu'une enquête visant à déterminer des vulnérabilités peut prendre du temps si le sujet est compliqué et nécessite des investigations complémentaires. Ce délai va encore être réduit avec les nouveaux équipements dont je vous ai parlé, probablement d'ici à l'été. Reste un délai supplémentaire pour la signature de l'habilitation, laquelle relève de la direction générale de l'armement (DGA), autorité d'habilitation pour les entreprises de la BITD.

Enfin, j'ai aussi mis en place un système de type « Chronopost », permettant aux demandeurs de savoir où en est leur dossier. L'officier de sécurité qui aura lancé la demande d'habilitation verra où elle se trouve. Si les gens veulent savoir, ils pourront ainsi s'adresser à la bonne personne.

S'agissant des interactions entre commande publique et souveraineté nationale, la DRSD est exemplaire puisque sa nouvelle base de souveraineté du service sera le premier système de contre-ingérence souverain ayant une véritable capacité « big data ». Lorsque j'ai

pris mes fonctions et que j'ai fait mon étude de marché, un autre service utilisait un système américain très connu. Avec la ministre, nous avons décidé que cela n'était pas possible et qu'il convenait d'en développer un français qui nous permette d'évaluer nos vulnérabilités et de les traiter nous-mêmes. C'est cette logique qui prévaut pour tous les systèmes que nous sommes en train de développer. Il en est ainsi pour le système de tri complexe pour les habilitations, que je viens d'évoquer, qui est purement français, élaboré avec des start-up françaises. Nous avons réussi à fidéliser un certain nombre d'entreprises, qui sont désormais sous contrat, avec lesquelles nous développons des systèmes français spécifiques, répondant exactement à notre besoin.

Nous partageons ces innovations avec les autres acteurs institutionnels. Ainsi, j'ai offert à l'ensemble de la communauté du renseignement notre nouveau système qui sera installé en 2021, opérationnel dans une première version en 2022 et susceptible de faire l'objet de développements ultérieurs. Certains services de renseignement ont déjà fait part de leur intérêt. La volonté de mutualiser existe donc. Nous essayons aussi d'acheter des équipements en commun et des systèmes nous permettant de communiquer entre nous et d'être plus efficaces même si, bien sûr, certains systèmes de renseignement sont spécifiques et nécessitent des développements particuliers.

S'agissant du Battle-Lab et des moyens de prévenir le risque d'espionnage, la problématique est la même que pour les salons d'armement. En temps normal – puisqu'en raison de la crise sanitaire, celui-ci a été annulé –, nous gérons la sécurité complète de celui du Bourget : nous nous occupons de la préparation, nous sommes présents pendant l'événement et gérons les retours d'expérience (RETEX) à l'issue. Nous proposons la même chose aux entreprises : quand un ingénieur ou une équipe part à l'étranger, nous les débriefons et les alertons sur les risques et les bons réflexes après le passage de la frontière – piratage du téléphone de service, de l'ordinateur dans la chambre d'hôtel, mise en sécurité des documents écrits, etc. Si nous sommes présents sur place, nous les accompagnons puis, au retour, nous faisons un bilan précis des événements, un RETEX, afin de mettre en lumière les éventuelles difficultés et, donc, les vulnérabilités. Quand on veut vendre, on s'expose et, quand on s'expose, le risque d'espionnage existe, d'où l'importance des mesures préventives, qui sont de notre ressort.

Je partage totalement l'analyse de M. Molins concernant l'arrêt Tele2 : nous allons être en difficulté si les fournisseurs d'accès ne sont plus obligés de garder en mémoire les connexions des douze derniers mois. On ne peut caractériser la menace que lorsqu'on a travaillé dessus. En outre, cela nous empêchera de connaître les comportements et les déplacements de la cible et nous devrons recourir à d'autres modes d'action, sans possibilité de gradation. Cette jurisprudence remet donc clairement en cause le fonctionnement des services de renseignement, la progressivité de nos opérations, leur préparation et la sécurité opérationnelle de nos personnels. C'est une catastrophe.

Je ne pense pas que les gens aient pleinement conscience de ce qui pourrait se passer, mais cela serait dramatique pour la sécurité en France. Tous les services de renseignement partagent le même avis : nous sommes en phase et nous en avons parlé au Président de la République. L'affaire suit maintenant un cours juridique.

La crise du Covid nous a amenés à adapter notre approche dans le cadre des inspections ou des entretiens avec les entreprises ou des personnels. Certains ne souhaitant

pas nous recevoir, nous avons fait une grande partie du travail par téléphone, ce qui nous a permis de développer des liens bénéfiques avec des salariés se sentant seuls et beaucoup d'entreprises qui n'avaient que nous comme contacts – nous sommes l'un des seuls acteurs à être resté quotidiennement au contact. Depuis septembre, les personnels de la DRSD travaillent en présentiel ; le télétravail est impossible car nos systèmes sont classifiés . Le travail à la maison n'est pas possible. Ils viennent donc travailler au Service avec des mesures barrières adéquates et des plages horaires étendues.

La *compliance*, dans les entreprises de la BITD, constitue une menace réelle. Pour obtenir du renseignement, il y a plusieurs moyens : le vol, par exemple, d'un ordinateur dans une chambre d'hôtel ou dans un train – c'est un cas très fréquent ; la séduction, en faisant rencontrer une prétendue âme sœur ; l'hameçonnage, par l'installation sur le téléphone ou la tablette d'un dispositif qui va récupérer les données. Mais tout cela demande un investissement, alors qu'il y a un outil plus simple par le droit : c'est le cas de la *compliance*. Il permet d'infliger des amendes record et de récupérer beaucoup d'informations légalement. D'ici peu, les seuls qui ne seront pas encore protégés, ceux dont le marché sera entièrement ouvert, ce seront les Européens.

Face à cette menace, notre rôle est d'alerter les entreprises et de faire en sorte qu'elles soient au niveau. Ainsi, la réglementation américaine sur le trafic d'armes au niveau international (ITAR) fixe les règles en matière de commerce des armes et ne cesse d'évoluer ; on ne sait jamais exactement ce qu'elle contient. Tout cela est très ciblé, au détriment des entreprises du secteur tout particulièrement.

La Chine est très présente. Ses entreprises sont très actives sur les technologies de pointe et la localisation de sites industriels appartenant à des entreprises chinoises près d'implantations sensibles militaires et civils exige des précautions qui seront au bénéfice des deux parties.

Quant à l'espionnage au profit de la Russie, il y a eu un cas récent en Italie et en France. Les services d'espionnage russes sont très actifs. L'actualité en témoigne.

La judiciarisation des faits est possible : c'est un autre service de renseignement qui s'en occupe, très souvent la DGSI. Nos relations avec les autres services sont parfaitement fluides, elles se renforcent et nous travaillons désormais ensemble que ce soit dans le domaine du terrorisme, de la sécurité économique ou du trafic d'armes. En la matière, nous ne cessons de progresser – je pense que cela apparaît en filigrane dans mon intervention. Les réseaux se développent, on partage de plus en plus d'expériences et de formations. L'Académie du renseignement joue un rôle important à cet égard.

En matière de cybersécurité, les collectivités territoriales ne font pas partie des attributions de la DRSD. Néanmoins, notre maillage territorial nous permet de disposer d'officiers experts en cybersécurité dans chacune des régions. Je leur ai demandé de se rapprocher des CERT, ces centres experts dans la réponse aux cyberattaques, qui sont en cours d'installation dans toutes les régions. Nous travaillons aussi avec les préfectures. Enfin, je l'ai dit, nous avons rejoint le GIP ACYMA, ce qui va nous permettre d'échanger des informations, d'affiner notre perception des menaces et de concevoir de meilleures parades. Ce sera à mon avis gage d'une meilleure efficacité encore à l'avenir. Nous allons en outre entrer en relation avec les entreprises qui seront certifiées ExpertCyber par le GIP ACYMA, afin de mieux coordonner les actions à leur niveau.

Cela étant, il n’existe pas de solution miracle. Il faut avant tout faire de la prévention, en permanence et à tous les niveaux, afin que les gens soient conscients des menaces. Nous intervenons ainsi auprès des Comex, des agents, des personnels qui partent en opération ou à l’étranger. Ensuite, il faut que nous ayons connaissance des menaces. Or les entreprises qui subissent des cyberattaques peuvent ne pas le dire pour ne pas nuire à leur réputation. Ce que nous essayons de faire, c’est de les aider à vaincre cette appréhension ; nous le faisons en développant notre réseau territorial et en établissant une relation de proximité, afin que les entreprises comprennent que nous sommes là pour les aider et non pour les sanctionner. Enfin, une fois que nous avons analysé une menace, il importe que nous puissions détecter le code malveillant puis vérifier que les entreprises qui disposent du même système ou ont accès aux mêmes réseaux ne font pas l’objet de la même menace.

À terme, les actions seront de mieux en mieux coordonnées entre le niveau national et les collectivités territoriales, mais cela requiert du temps. La priorité, aujourd’hui, est de développer les compétences : on manque de cyberdéfenseurs. Les besoins ne cesseront de croître dans les prochaines années et on va avoir besoin d’une armée de cybercombattants.

La loi de 2015 est une bonne loi, car elle protège à la fois nos agents et le citoyen, et offre en cela un bon équilibre. Elle permet de nous inscrire dans le même cadre que nos partenaires internationaux. À mon sens, les modifications à lui apporter seraient minimes. On pourrait, par exemple, envisager une harmonisation des délais légaux pour certaines techniques de renseignement. Je souhaiterais néanmoins que nous continuions sur notre lancée, parce que nous avons mis beaucoup de temps pour appréhender le nouveau système. Il serait bon d’avoir un peu de stabilité. La loi est d’application récente : cinq ans, ce n’est pas très long pour un texte qui a nécessité trois à quatre années de conception. Nous sommes dans les faits très contrôlés.

La prolifération nucléaire fait l’objet d’un suivi de la part des services partenaires ; cela ne fait pas partie de mes compétences directes.

Concernant la radicalisation, une enquête a été menée à la suite de l’attentat d’octobre 2019 à la direction du renseignement de la préfecture de police de Paris. Elle a montré que le système de la DRSD était efficace. Premièrement, tous ceux qui veulent nous rejoindre en tant que militaires sont passés au crible, et notre méthode de criblage ne cesse de se perfectionner. Deuxièmement, ce que nous appelons le commandement, à savoir l’encadrement de proximité, permet de détecter les changements de comportement. En cas d’anomalie, le référent du régiment nous contacte et nous allons immédiatement voir ce qu’il en est. Nous menons des enquêtes à charge comme à décharge ; par exemple, nous avons eu le cas d’une femme qui avait accusé son mari de s’être radicalisé, mais c’était faux : il s’agissait d’une vengeance dans le cadre d’un divorce. Cette rapidité de détection et de réaction fait notre force, même s’il convient de rester humble.

Nous n’avons pas de difficulté à recruter. Pour les personnels civils, nous recevons environ trente candidatures pour un poste – quoique pour certains très spécialisés, le rapport soit plutôt de deux pour un, voire d’une pour un.

S’agissant de la mouvance d’ultradroite, je le répète, nous passons au crible tous les personnels militaires qui souhaitent rejoindre nos services, au moyen de ce que nous appelons l’enquête initiale de sécurité. L’objectif est de vérifier qu’il s’agit de personnes loyales envers

le drapeau et la République. Nous avons procédé à 311 000 enquêtes cette année et à plus de 370 000 l'année dernière – la diminution étant liée à l'épidémie de covid-19. Pour l'heure, nous n'avons pas légalement la possibilité d'en faire une de manière préalable au recrutement pour les personnels civils, mais nous essayons d'y remédier, car lorsqu'il s'avère que quelqu'un qui a été recruté est radicalisé, on n'a guère de solution. Nous travaillons ce sujet avec la secrétaire générale pour l'administration (SGA).

Si l'enquête conclut à la possibilité d'un recrutement, la personne est jugée apte pour le service et nous ne le suivons plus s'il ne fait pas l'objet d'une procédure ou de nouvelle demande d'habilitation. Il faut que quelqu'un fasse un signalement pour que nous puissions intervenir ultérieurement. Je précise que sur les cinquante cas relevés par Mediapart, quarante-deux appartenaient à la Légion étrangère, qui effectue son propre recrutement à l'aide d'un service dédié. Tous ne sont plus en activité. Des sanctions ont été prises et le problème est en cours de traitement. Cela étant, je rappelle que la Légion étrangère offre à certains une deuxième chance. Certaines des personnes engagées antérieurement dans cette mouvance n'ont eu aucune activité en la matière depuis qu'elles ont rejoint l'armée. Les assertions de Mediapart ne sont donc pas toutes confirmées par la Légion étrangère.

Les sept autres cas sont en cours de traitement par l'armée de Terre. Cela représente en définitive un nombre très faible d'individus, même si c'est une atteinte grave à la réputation des armées, que la ministre a dénoncée avec beaucoup de fermeté. Nous n'avons pas la volonté de garder dans nos rangs ces personnes qui ont failli à leur devoir de neutralité et n'ont pas respecté l'engagement qu'elles avaient pris.

S'agissant des fuites de données, il faut avoir à l'esprit qu'avec les dossiers partagés, on peut obtenir très rapidement beaucoup d'informations ; une fois volés, ces dossiers sont mis sur des plateformes et vendus. Beaucoup de nos adversaires cherchent à récupérer des données médicales.

Les ONG sont-elles instrumentalisées ? Ce qui est sûr, c'est que certaines, notamment panafricaines, qui agissent contre nos opérations extérieures, sont financées par des puissances étrangères. Et je pense que lorsqu'une ONG bloque un port français pour empêcher l'exportation d'armes, il y a un intérêt économique derrière – la difficulté étant de le prouver. Si les militants agissent en toute innocence, avec naïveté, les financements, eux, proviennent parfois de puissances qui œuvrent contre les intérêts de la France.

Mme la présidente Françoise Dumas. Merci, général, pour ces explications. Je retiens de votre intervention trois points saillants.

Le premier est l'accentuation des menaces d'ingérence économique.

Le deuxième, ce sont les conséquences de l'arrêt Tele2, que nous suivons de très près – nous avons d'ailleurs organisé la semaine dernière, avec la commission des affaires européennes, une table ronde sur le sujet. Nous saurons être à vos côtés si nécessaire, mais, pour l'heure, nous ne pouvons pas faire grand-chose, sinon espérer que la Cour de justice saura, en la matière, être pragmatique et non dogmatique.

Le troisième point est la protection, avec la transformation de la DRSD et le nécessaire renforcement de ses effectifs, de ses moyens et de ses techniques – ce qui nous concerne tous,

dans nos circonscriptions. Nous aurions tout intérêt à mobiliser les services de l'éducation nationale et ceux du ministère de l'enseignement supérieur, de la recherche et de l'innovation pour développer sur l'ensemble du territoire national les compétences nécessaires. Nos talents sont très demandés en France, tant par le secteur civil que par le militaire, mais ils peuvent être aussi pillés ou attirés par d'autres cieux.

Sachez, général, que nous sommes à votre disposition et que les parlementaires ont été attentifs à vos remarques et à l'expression de vos besoins.

*

* *

La séance est levée à dix-neuf heures dix.