M. le président Thomas Gassilloud. Nous avons le plaisir d'accueillir le général Philippe Susnjara, directeur du renseignement et de la sécurité de la défense (DRSD) depuis octobre 2022. C'est la première fois, mon général, que nous vous auditionnons en cette qualité. Saint-Cyrien passé par les troupes de marine, vous avez notamment été adjoint au centre de planification et de conduite des opérations (CPCO) de l'état-major des armées en 2018 avant d'en prendre la direction deux ans plus tard.

Lors de ses vœux aux forces armées, le Président de la République a annoncé un doublement des crédits de la DRSD dans le cadre de la loi de programmation militaire (LPM). J'imagine que vous ne manquerez pas de revenir sur cette augmentation substantielle des crédits dans un contexte où les défis à relever sont nombreux pour la DRSD : recrutement et fidélisation des personnels civils et militaires ; réaménagement de la direction centrale au fort de Vanves ; développement de nouveaux systèmes d'information souverains ; contre-ingérence économique et contre-ingérence cyber à l'heure de l'économie de guerre et de l'explosion du nombre de signalements d'intrusions cyber.

N'hésitez pas, dans votre introduction, à rappeler les missions de la DRSD car la commission a été fortement renouvelée lors des dernières élections législatives.

Général de corps d'armée Philippe Susnjara, directeur du renseignement et de la sécurité de la défense. Je suis extrêmement honoré d'être parmi vous pour présenter la DRSD. Cette direction est le service de renseignement du ministre des Armées chargé d'assurer la protection des installations, des personnes, des systèmes, des matériels et des informations du ministère. Le champ de compétences de la direction couvre la sphère de défense élargie, à savoir le ministère des armées et les personnels qui y servent, mais aussi les familles, les anciens militaires, les réservistes et la base industrielle et technologique de défense (BITD), composée d'environ 4 000 entreprises.

La mission du service est contenue dans sa devise, *« Renseigner pour protéger »*. Notre action comporte en effet deux volets : le premier, de renseignement, consiste à collecter et à analyser des informations et le second vise à améliorer la protection de la sphère de défense élargie. Le travail repose sur trois piliers : évaluation de la menace, identification des vulnérabilités – physiques, cyber, des personnels –, puis estimation, reposant sur le croisement des deux premières tâches, d'un niveau de risque, acceptable ou non. Si le niveau de risque nous semble inacceptable, nous réfléchissons au déploiement de mesures destinées à le diminuer ou à entraver toute ingérence.

Pour remplir ces missions, notre organisation est très centralisée, puisque tout remonte à la direction centrale, située au fort de Vanves à Malakoff ; nous possédons en outre une particularité que nous partageons avec nos camarades de la direction générale de la sécurité intérieure (DGSI), à savoir une implantation locale : la direction compte ainsi huit directions zonales constituées de cinquante-six postes répartis dans l'Hexagone, outre-mer, à l'étranger où nous avons des forces prépositionnées et aux côtés des forces en opération.

La DRSD poursuit sa transformation engagée depuis plusieurs années et accélérée ces derniers temps. Nos effectifs ont crû et nous avons retrouvé, en 2021, le niveau d'avant la période

2008-2014, à savoir 1 550 personnels. Toujours dans le domaine des ressources humaines, de nouveaux métiers se sont implantés dans la direction : cyber ; développeurs informatiques ; jeunes agents civils, que l'on appelle les agents de contre-ingérence économique et qui agissent en complément des inspecteurs de la sécurité, qui sont, eux, plutôt des personnels militaires. Nous nous adaptons en permanence aux nouvelles technologies pour relever, avec nos camarades du premier cercle, les nombreux défis de ce domaine. Enfin, nous avons conduit une transformation capacitaire, la plus emblématique étant le développement d'une nouvelle base de données souveraine, qui doit se substituer à notre système vieillissant à partir de 2024.

Ces multiples évolutions se sont déployées dans le cadre de la LPM en cours. Entre 2019 et 2025, la direction a reçu 120 millions d'euros en crédits de paiement (CP) ; les révisions annuelles nous ont alloué 219 millions de CP pour conduire nos nouveaux projets : la nouvelle base de données souveraine ; l'acquisition de nouvelles capacités cyber ; l'adaptation à la nouvelle instruction générale interministérielle, IGI 1 300, sur la protection ; la conception puis la construction du nouveau bâtiment au fort de Vanves, qui sera livré à la fin de l'année 2024 et qui accueillera à partir de 2025 l'ensemble des personnels du cœur de métier de la direction ; l'amélioration du système d'enquêtes administratives de renseignement et de sécurité, en développant de nouveaux outils comme l'empreinte numérique finalisée,; l'amélioration, enfin, de notre système d'information dédié aux habilitations – synergie pour l'optimisation des procédures d'habilitation de l'industrie et des administrations (Sophia).

Les ressources qui nous ont été allouées ont eu un effet direct sur les missions du service, dans un contexte tendu sur le front des menaces. En plus des risques traditionnels liés au terrorisme, nous assistons à une résurgence, déjà soulignée dans la revue nationale stratégique (RNS) de 2017 et amplifiée par le conflit en Ukraine, des États-puissances, laquelle accroît le coût de la menace. Nous avons enregistré une augmentation spectaculaire des demandes liées à la protection, puisque nous en avons reçu 390 000 en une année, soit 1 500 à 1 800 par jour : ces demandes vont de contrôles simples de personnes devant entrer dans une base ou une zone réservée à des habilitations de personnes devant avoir accès à des documents très secrets. La hausse des sollicitations est constante depuis plusieurs années, avec des accélérations lors des périodes d'attentat ; nous tenons les délais qui nous sont fixés, mais y parvenir représente un défi quotidien ; nous souhaitons donc automatiser le plus possible ce processus, afin que les agents de la direction puissent effectuer des enquêtes de qualité, à charge et à décharge. En 2022, nous avons mené en outre 155 inspections en milieu militaire et industriel, destinées à vérifier le niveau de protection de ces installations et leur conformité avec la réglementation.

Nous avons effectué près d'un millier de sensibilisations du personnel du ministère des armées et de la BITD : ces actions sont la base de la réussite de notre mission car, quand les gens sont sensibilisés, ils font attention et ils évitent de commettre certaines erreurs. Si jamais un événement se produit, ils sont capables de nous en informer pour évaluer la situation et prendre les mesures nécessaires.

Notre production de notes de renseignement a, elle aussi, augmenté, de l'ordre de 19 % en quatre ans.

Dans le cadre de la préparation de la nouvelle LPM pour les années 2024 à 2030, nous avons conduit, à notre niveau, une sorte de revue stratégique, dans laquelle nous nous sommes penchés sur les évolutions des six à sept prochaines années. Nous avons identifié quatre axes d'effort. Le premier concerne l'adaptation, dans le domaine de la contre-ingérence, aux nouvelles conflictualités, principalement liées aux États intrusifs, au premier rang desquels figurent la Russie et la Chine. Le deuxième consiste à répondre à la forte progression des actions hostiles à la BITD ; le contexte économique et géopolitique actuel montre que cette tendance est appelée à durer. Le troisième vise à poursuivre notre montée en puissance cyber et à nous adapter aux bouleversements technologiques à venir. Le quatrième, enfin, tient à l'exigence de ne pas baisser notre garde face aux menaces des dernières années, principalement le terrorisme et la radicalisation.

Premier axe, l'invasion de l'Ukraine par la Russie a profondément marqué le cadre géopolitique actuel. Elle a tout d'abord confirmé la désinhibition de certains États à conduire des actions violentes ; ceux-ci sont prêts à employer de multiples moyens, et un conflit de haute intensité en Europe est possible. Avec cette agression, la Russie est entrée dans la catégorie des nations hostiles, au moins à court et à moyen terme et dans notre domaine d'action. Les conséquences sont multiples mais assez prévisibles : les tentatives d'ingérence russes vont se multiplier, notamment à l'encontre de nos institutions et des armées européennes ; l'Otan va revenir au premier plan, puisque la totalité de nos partenaires se tournent vers cette organisation ; enfin, les questions de sécurité et de défense vont connaître un regain d'intérêt dans l'ensemble des pays occidentaux, notamment européens. L'ingérence russe s'étend partout, notamment en Afrique : au-delà des actions traditionnelles qui se situent en dessous du seuil de conflictualité – espionnage, manœuvres de déstabilisation et d'intimidation –, nous subissons des contestations à visage découvert. Il n'y a qu'à écouter Evgueni Prigojine, chef de la société militaire privée (SMP) Wagner, qui assume d'agir contre les intérêts français, notamment en animant des réseaux dans le champ informationnel. Dans ce domaine, notre priorité est d'accompagner les forces déployées sur le terrain pour qu'elles puissent conduire correctement leurs opérations sans subir d'actions d'ingérence ; nous recueillons du renseignement pour participer à la protection de nos forces ; nous avons ainsi accompagné ces dernières lors de leur retrait du Mali et du Burkina Faso ; nous restons aux côtés des forces prépositionnées au Sénégal, au Tchad, au Gabon et à Djibouti et des forces en opération au Niger et au Tchad. Nos compétiteurs stratégiques, principalement la Chine et la Russie, disposent de moyens puissants, variés et sophistiqués qui nous obligent à conserver la capacité de traiter et d'exploiter les données – la « guerre de la donnée » n'est pas une vaine expression – et à posséder un temps d'avance. Pour la nouvelle LPM, nous avons mis en avant la nécessité de poursuivre le développement de notre nouvelle base de données souveraine pour y inclure certains outils qui nous permettent de traiter les données, de mettre en relation des signaux faibles, de déterminer des schémas d'attaque d'adversaires, de mieux orienter nos capteurs et de mieux conseiller la BITD et les forces pour renforcer leur protection. Nous réfléchissons également au développement d'un arsenal normatif à même de prévenir les ingérences étrangères ; dans cette optique, nous avons travaillé au renforcement du contrôle déontologique des militaires, anciens et actuels, afin d'éviter la fuite de savoir-faire, comme la presse s'en est fait l'écho ces dernières semaines au sujet des pilotes de chasse.

Le deuxième axe touche aux actions hostiles contre la BITD. Les tentatives de prédation et de

déstabilisation de la base industrielle et technologique de défense se sont multipliées. Elles prennent la forme d'ingérences légales, au travers des normes et de la réglementation, ou extralégales, avec, par exemple, des attaques contre la réputation d'une entreprise concourant à un marché, des captations d'informations, l'affaiblissement d'un concurrent, etc. L'augmentation du budget de la défense et la mise en avant des matériels occidentaux aiguisent certains appétits. Dans ce domaine, la Chine représente la menace principale : elle agit dans de nombreux secteurs, pas uniquement celui de la défense, et se montre particulièrement intrusive dans la recherche. Nous devons nous montrer vigilants sur les normes et les réglementations, notamment anglo-saxonnes, car la Chine et d'autres pays souhaitent se doter de moyens importants en la matière ; la DRSD travaille très étroitement avec Tracfin et la DGSI, services avec lesquels nous avons des contacts hebdomadaires. Dans le cadre de l'économie de guerre, nous avons identifié avec la direction générale de l'armement (DGA), au-delà des entreprises connues possédant des savoir-faire particuliers, les petites et moyennes entreprises (PME) de la chaîne logistique qui peuvent constituer une cible pour nos adversaires. À cet égard, notre objectif est de se doter d'un outil utilisant la cartographie en 3D et la technologie des jumeaux virtuels pour disposer d'une meilleure vision de l'ensemble des installations et d'une connaissance en temps réel et à jour de nos niveaux de protection.

Le troisième axe a trait à la montée en puissance du cyber. La croissance de la virtualisation de la vie économique augmente naturellement le niveau de risque cyber, principalement pour les PME dont la capacité à se doter d'outils de défense est plus faible que celle des grosses sociétés. Nous travaillons beaucoup avec ces entreprises, en lien avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) et le commandement de la cyberdéfense (Comcyber), avec lequel nous avons développé une coopération renforcée. Dans notre direction, des équipes techniques de réponse aux attaques cyber sont centrées sur l'économie de défense, quand le Comcyber s'occupe du ministère des armées. Nous devons être à jour des capacités modernes – objets connectés, 5G, intelligence artificielle, etc. –, qui nécessitent des moyens toujours plus sophistiqués pour être à la pointe des avancées technologiques.

Le dernier axe concerne le terrorisme et la radicalisation. Notre feuille de route est claire : ne pas baisser la garde. Nous avons développé de nombreuses actions de coopération efficaces entre les services du premier cercle et avec le commandement des différentes armées. Le risque existe, mais il est connu et contenu. Nous devons rester vigilants sur les évolutions de la menace, y compris celles provenant d'autres fragmentations sociales et du séparatisme. Sur ce dernier point, tout ce qui nous permet de savoir ce qui se passe sur les réseaux sociaux est intéressant, puisque les personnes, notamment les jeunes, échangent énormément sur ces réseaux et très peu sur l'internet classique : nous devons nous adapter à ces nouveaux moyens de communication.

Pour atteindre nos objectifs dans ces quatre domaines, nous devons, comme les autres services de renseignement, relever le défi des ressources humaines, à savoir conquérir de nouveaux talents et les garder quelque temps pour tenir les délais. Nous souscrivons à tous les efforts que la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) a engagés pour coordonner notre action dans le domaine des ressources humaines et nous participons activement à tous les travaux en cours. Grâce à la sous-direction « stratégie

et ressources » et à un effort quotidien, nous avons tenu nos engagements pour le recrutement de nos agents et nous sommes à environ 97 % de l'effectif autorisé. Il s'agit d'un combat quotidien, d'autant que la jeunesse de nos agents crée un flux permanent dans nos effectifs. Nous insistons sur la création de nouveaux métiers et sur la diversification de nos viviers, tout en étant conscients du fait que l'augmentation des effectifs de la direction est principalement due à l'arrivée de civils, parce que les armées peinent à maintenir le nombre de militaires au sein de la direction. Nous suivons des pistes pour trouver de nouveaux profils de militaires. Mon prédécesseur a engagé des actions dans le domaine de la formation et des parcours professionnels, lesquelles seront poursuivies avec la volonté de mettre en place un centre de formation, qui nous sera utile car 700 de nos agents reçoivent chaque année une formation ; nous voulons proposer des formations certifiantes, qui valorisent nos personnels. Dernier point, le nouveau bâtiment de la direction centrale offre au service l'opportunité de se réorganiser en mettant en adéquation l'espace géographique des bureaux et les processus internes de la direction. Un grand travail nous attend pour exploiter au maximum toutes les capacités du nouveau bâtiment du fort de Vanves et accomplir notre mission de mieux renseigner pour mieux protéger.

M. Jean-Michel Jacques, rapporteur. J'ai eu la chance de visiter la DRSD centrale et locale, la direction comptant une antenne dans le pays de Lorient. Je vous remercie de l'accueil que j'y ai reçu. Comme mes collègues députés, j'ai participé à des événements avec les entreprises qui travaillent dans l'écosystème de la défense et j'ai trouvé très intéressant de me connecter avec vous pour que tous les membres de l'équipe France se rencontrent, car de nombreuses entreprises locales ne sont pas forcément sensibilisées à l'ingérence : nous, parlementaires, devons les aiguiller vers vous.

Vous avez laissé entendre que vous aviez plus de difficultés à attirer des militaires que des civils : comment pouvez-vous agir, surtout avec la contrainte des opérations extérieures (Opex) ? Que faire pour augmenter l'attractivité de votre direction auprès des militaires ?

Le projet de LPM prévoit 5 milliards au renseignement : la part qui reviendra à la DRSD vous paraît-elle adaptée aux objectifs de votre service ? Quels investissements bénéficieront en priorité de cette enveloppe ?

Général de corps d'armée Philippe Susnjara. J'attache une grande importance à l'équilibre entre personnels militaires et civils : notre spectre d'action couvre à la fois les forces et la BITD, donc nous devons maintenir un niveau de personnels militaires suffisant, d'autant que nous accompagnons les forces dans les Opex. Actuellement, nous comptons 63 % de militaires et 37 % de civils : il faut conserver, à un ou deux pourcent près, cette répartition.

Le problème ne tient pas tant à l'attractivité du service, même si la question se pose toujours, qu'à la nature des profils : les personnels militaires qui nous rejoignent sont souvent en deuxième voire en troisième partie de carrière – sous-officiers et officiers comptant une quinzaine d'années de service. Or l'armée souffre d'un creux conjoncturel, qui rend difficile l'occupation de tous les postes. Nous souhaitons donc sélectionner des personnes aux profils légèrement différents, notamment plus jeunes : je discute actuellement avec mes camarades des armées pour prendre ce virage, qui demandera plus de formations mais qui augmentera la durée d'occupation des postes. S'agissant des Opex, nous ne déplorons pas de manque

d'agents, même si nous surveillons les taux de tour.

En fonction du budget qui nous sera alloué, nous souhaitons maintenir notre effort sur la base de souveraineté: la version, qui est appelée à remplacer la base actuelle, devrait être livrée et opérationnelle mi 2024 –. Nous souhaitons incrémenter cette base de données avec des outils, des modules et des briques qui l'enrichissent : insérer du prédictif, traiter les signaux faibles, rapatrier toutes nos données dans une seule base, effectuer des recherches dans l'ensemble de nos données sont des éléments essentiels pour nous. Voilà l'effort prioritaire que nous fournissons, ce processus ne pouvant de toute façon pas être suspendu.

Nous souhaitons également améliorer les outils en place dans le cadre du Centre national des habilitations de la défense (CNHD) : nous devons automatiser et industrialiser les enquêtes administratives afin que les agents puissent consacrer toute leur énergie aux dossiers qui réclament de l'intelligence humaine. Pour ce faire, nous allons développer de nouveaux outils, qui ne sont pas forcément très complexes puisqu'il s'agit de mettre en relation les différentes boîtes qui existent déjà. Notre objectif est double : lisser les processus et améliorer notre consultation des réseaux sociaux, en employant peut-être des modules de traduction.

Enfin, nous cherchons à améliorer les conditions de travail de nos agents ainsi que la qualité de la performance, notamment dans l'utilisation d'outils nomades qui doivent nous faire gagner du temps et dans l'élaboration d'un système centralisé qui nous offre une vision plus globale et plus rapide.

Mme Anne Genetet (RE). Je comprends que vous n'avez pas encore d'idée précise de la répartition des 5 milliards et j'imagine que vous aimeriez capter une part importante de l'augmentation de 60 % de l'enveloppe consacrée au renseignement. Vous souhaitez moderniser certains de vos outils, mais cela dépendra, là aussi, des crédits qui vous seront alloués. Connaissez-vous le calendrier de ventilation du budget du renseignement ?

L'article 20 de la LPM garantit la prise en compte des intérêts fondamentaux de la nation : quand un ancien militaire veut rejoindre le secteur privé, comment se prémunir de l'ingérence d'une puissance étrangère ? La rédaction actuelle de l'article 20 vous semble-t-elle suffisante pour vous prémunir de départs d'agents, civils comme militaires, vers les conseils d'administration d'entreprises étrangères ?

Général de corps d'armée Philippe Susnjara. Je ne connais encore ni le cadrage, ni l'arbitrage budgétaire : nous avons identifié des priorités, que nous mettrons en œuvre en fonction de l'arrivée des crédits.

Mme Anne Genetet (RE). Les menaces que vous avez évoquées sont multiples, hybrides et évolutives ; elles requièrent de votre part une grande agilité et réactivité, et j'imagine que, dans ce contexte, vous nourrissez sûrement des ambitions, des objectifs, des exigences, des attentes, des impatiences.

Général de corps d'armée Philippe Susnjara. Bien sûr, mais les menaces étant infinies, nos capacités seront théoriquement toujours insuffisantes. Voilà pourquoi nous devons définir des priorités et optimiser les moyens dont nous disposons. Actuellement, la priorité va

clairement à la base de données souveraine. Ensuite, nous voulons développer quelques capacités très particulières dans le domaine du cyber : quel que soit le montant de notre budget, nous avancerons dans ce domaine. Enfin, nous ajusterons dans le temps nos efforts de déploiement d'autres capacités suivant les crédits qui nous seront alloués.

Si l'un de nos agents veut quitter notre service pour occuper un emploi le mettant en contact avec l'étranger, nous souhaitons qu'il fasse une déclaration préalable pour que nous sachions si ce changement présente ou non une menace. Notre contrôle devrait ressembler aux enquêtes d'habilitation : nous évaluerons l'environnement de l'individu et les sujets qu'il aura à traiter pour déterminer l'existence d'un risque d'ingérence. Il y aura des avis complémentaires, l'ensemble permettant au ministre de décider si l'agent peut partir ou non à l'étranger. Nous pourrons prendre des sanctions si les individus ne tiennent pas compte de l'avis. Cette mesure d'entrave n'existait pas précédemment.

M. Pierrick Berteloot (RN). La récente acquisition de l'entreprise Exxelia par le groupe américain Heico est la dernière cession en date de l'un de nos champions industriels. Cette entreprise fournit des composants électroniques aux nouveaux sous-marins nucléaires d'attaque (SNA) Barracuda, aux Rafale, aux lanceurs Ariane 5 et 6 et à l'Airbus A320neo. La PME française Segault est également en passe d'être rachetée par le groupe texan Flowserve, alors qu'elle possède une expertise mondiale dans les systèmes de robinetterie et de chaufferie nucléaire ; elle équipe les centrales nucléaires françaises, le porte-avions Charles-de-Gaulle et son successeur, les SNA et les sous-marins nucléaires lanceurs d'engins (SNLE) ; elle fournit aussi les systèmes de sûreté des missiles nucléaires M51. Il n'est donc pas abusif d'affirmer que cette entreprise est stratégique pour notre armée : sa vente soulève de très nombreuses craintes légitimes et révèle l'atteinte à nos intérêts économiques et stratégiques, laquelle ne semble pas devoir s'arrêter pour le moment.

La protection de ces intérêts est pourtant une préoccupation de l'État : la défense et la promotion de l'économie française figurent en bonne place dans la stratégie nationale du renseignement, dans laquelle on lit que « Le premier objectif de notre politique de sécurité économique est de détecter et de neutraliser le plus en amont possible toute menace sérieuse, potentielle ou avérée, systématique ou ponctuelle, susceptible d'affecter les intérêts économiques, industriels et scientifiques » de la nation. La DRSD participe activement à prévenir la fuite de nos savoir-faire et à entraver l'ingérence de certains acteurs étrangers ; or toutes ces cessions d'entreprises françaises à des sociétés américaines créent un sérieux risque d'atteinte à notre souveraineté et à nos informations hautement sensibles.

La DRSD étant chargée de la protection des sites industriels sensibles de défense comme de la prévention des fuites, comment s'organise-t-elle face aux intrusions d'alliés certes importants, mais qui n'hésitent pas à nous espionner et à accroître leur contrôle sur nos industries de défense ?

Général de corps d'armée Philippe Susnjara. Il s'agit effectivement du cœur de notre métier dans le domaine de la contre-ingérence économique. Plusieurs bureaux à la direction centrale veillent à la sécurité économique ; les postes locaux sont en relation avec les industries de leur ressort. Les 4 000 entreprises de la BITD voient au moins une ou plusieurs fois par an, selon leur degré de sensibilité, nos agents. Notre mission est de garantir la

protection physique et cyber de l'entreprise en nous assurant qu'il n'y ait pas d'intrusion et de recueillir des informations sur de possibles cessions. Comme la DGSI, nous faisons remonter ces informations pour présenter les menaces qui peuvent peser sur une société du fait de prises d'intérêts ; nous n'avons pas la connaissance fine de la sensibilité de certaines compétences, si bien que nous travaillons avec la DGA ; la situation de l'entreprise que vous avez évoquée est évidemment connue, mais la DGA sait s'il existe ou non des alternatives et si la conservation d'un composant est vitale pour notre autonomie stratégique. Le secrétariat général de la défense et de la sécurité nationale (SGDSN) conduit un travail interministériel, notamment avec le service de l'information stratégique et de la sécurité économiques (Sisse) du ministère chargé de l'économie. Dans ce cadre, nous nous interrogeons sur l'existence d'une menace réelle et sur les mesures à prendre, mais la DRSD n'a pas de levier sur ces dernières.

M. Aurélien Saintoul (LFI-NUPES). Mon collègue a été un peu pudique en ne vous demandant pas quelle était l'appréciation de votre service sur la possible cession de Segault. Je mets les pieds dans le plat : que pense la DRSD de cette vente ?

La DGSI signale depuis quelque temps l'extrême droite comme l'une des principales menaces contre la sécurité intérieure. Qu'en est-il du point de vue de la DRSD ?

La contre-ingérence économique couvre aussi la préservation du patrimoine intellectuel du pays : quels sont les moyens et la présence de votre service dans l'enseignement supérieur ?

Dans la fuite de documents confidentiels du gouvernement américain dans le New York Times, la France n'apparaît pas comme une cible de l'espionnage des États-Unis – ce fait étant de notoriété publique depuis bien longtemps –, mais j'aimerais connaître votre appréciation de cet événement. L'entourage du ministre des armées a contesté les faits avancés dans les documents : considérez-vous ces fuites comme une manipulation ?

Le directeur général de la sécurité extérieure (DGSE) nous a dit que le budget de son service allait approcher les 5 milliards, ce qui ne laisse pas grand-chose aux autres. Qu'en est-il du vôtre ?

M. le président Thomas Gassilloud. La LPM prévoit un effort budgétaire de 5 milliards, et la DGSE recevra un budget de l'ordre de 5 milliards sur l'ensemble de la période couverte par la LPM, mais heureusement que la DGSE ne consommera pas l'intégralité de l'effort consenti dans la LPM. Le DGSE laissait sous-entendre qu'il estimait à due proportion la répartition de ces 5 milliards d'euros, mais je suppose que les autres services, dont la DRSD, diront qu'ils ont besoin d'un rattrapage en termes de crédits. Il ne faut pas confondre le budget annuel et le budget sur l'ensemble de la période de la LPM.

M. Aurélien Saintoul (LFI-NUPES). Le plus simple serait que vous exprimiez clairement votre besoin puisque les arbitrages n'ayant pas encore été rendus, les parlementaires ont la possibilité de conclure les discussions qui se tiennent au sein de l'exécutif.

Général de corps d'armée Philippe Susnjara. Nous avons évalué la sensibilité de la cession de l'entreprise Segault, sous l'angle de la menace éventuelle pesant sur certains des

programmes que nous déployons avec la BITD. Je ne suis pas en mesure de dire s'il y a un danger majeur, mais j'ai défendu l'idée qu'il y avait un problème et qu'il était important de se saisir du sujet ; celui-ci est bien pris en compte, mais ce sont les gens spécialisés dans le domaine des armements qui peuvent répondre à la question de l'acceptabilité du risque. Dans ce processus, je n'évalue qu'une partie du risque.

Nous travaillons avec la DGSI pour améliorer la protection des laboratoires et des instituts de recherche scientifiques : nous nous répartissons les laboratoires, certains n'étant suivis que par la DRSD, d'autres relevant de la surveillance de notre direction et de la DGSI. L'action prioritaire est la sensibilisation : c'est une démarche essentielle car le monde de la recherche et la protection sont antinomiques, puisque la recherche suppose l'ouverture vers l'extérieur, l'échange et la publication quand la protection pousse à la fermeture et au mutisme. Nous ne sommes pas là pour empêcher les publications, mais nous sensibilisons les acteurs de la recherche à l'identification de la menace et de nos vulnérabilités ; ensuite, il convient de déterminer où l'on place le curseur entre ouverture et fermeture. Ces trois dernières années, les personnes travaillant dans les laboratoires de recherche ont modifié leur appréhension du sujet car, il y a encore quelque temps, elles ne voulaient pas entendre parler de protection ; certains épisodes malheureux ont joué un rôle dans cette prise de conscience.

D'une manière générale, nous suivons l'ensemble de la radicalisation, qui se développe malheureusement dans la société actuelle. Nous avons connu des radicalisations islamistes extrêmement rapides à cause des réseaux sociaux, et nous retrouvons actuellement ce processus pour l'ensemble des groupes radicaux, qui s'autoalimentent et développent un caractère quelque peu sectaire. Nous suivons la présence de l'ultradroite au sein des armées, mais il n'y a pas de sujet particulier ; nous prenons les mesures d'entrave, en lien avec le commandement, lorsqu'elles sont nécessaires – nous agissons de la même façon avec l'islam radical. Pour l'ultragauche, la situation est opposée puisque nous avons plutôt affaire à des gens qui pourraient viser la BITD ou les institutions de l'extérieur : là, nous travaillons de manière coordonnée avec les autres acteurs du renseignement.

J'ai des équipes qui suivent les fuites du New York Times, mais il est très difficile de se prononcer actuellement car on décèle certaines manipulations : il y a ainsi des documents-miroirs, certains donnant, par exemple, des chiffres de pertes favorables aux Ukrainiens, d'autres aux Russes. La diffusion de ces documents est parfois une simple photographie, donc il faut vérifier leur véracité : existent-ils réellement ? Certains d'entre eux sont des appréciations du partenaire américain. Nous suivons ce dossier, mais l'affaire est un peu récente pour que nous puissions nous positionner, sachant que, comme tout service de renseignement, nous sommes un peu paranoïaques et nous tentons de voir toutes les faces d'une information.

Avec la LPM actuelle, nous sommes arrivés à un plateau budgétaire, hors infrastructures, de 20 millions d'euros, donc nous sommes assez modestes. Une progression est prévue, et nous aimerions atteindre environ 30 millions d'euros en plateau à la fin de la prochaine LPM. Ces ordres de grandeur diffèrent profondément de ceux de la DGSE, mais cela a toujours été le cas et je n'en veux pas du tout au DGSE. Nous sommes un petit service.

M. le président Thomas Gassilloud. Hors infrastructures, votre budget représente environ

10 % de celui de la DGSE, n'est-ce pas ?

Général de corps d'armée Philippe Susnjara. Oui, à peu près.

Mme Delphine Lingemann (Dem). Au nom du groupe Démocrate, je vous remercie pour vos explications sur les enjeux auxquels fait face la DRSD. L'une de vos missions est de mener des opérations de contre-ingérence dans la sphère de la défense avec pour objectif de protéger nos forces armées, la BITD et le cyberespace. Votre activité est donc très liée à la guerre d'influence. Lors de la présentation de la RNS en novembre dernier, le Président de la République a érigé l'influence en sixième fonction stratégique des armées françaises. C'est la preuve que le domaine informationnel est devenu un champ de bataille, qui fait désormais partie des nouveaux espaces de conflictualité que nos armées doivent maîtriser d'ici à 2030.

Alors que votre rôle est de déceler et d'entraver toute menace externe susceptible de porter atteinte à l'institution militaire, à une entreprise de la BITD ou à un laboratoire de recherche, quelle stratégie la DRSD compte-t-elle déployer, dans la période de la LPM, dans le domaine de la guerre d'influence ?

Lors d'une audition de la commission d'enquête sur les ingérences de puissances étrangères, le directeur du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a expliqué le fonctionnement de son service. Coopérez-vous avec lui dans le cadre de votre mission de contre-ingérence cyber ?

L'intelligence artificielle se trouve au cœur des enjeux de cybersécurité, secteur qu'elle est sur le point de révolutionner compte tenu de sa capacité à analyser des masses considérables de données. Pouvez-vous nous donner des précisions sur l'intégration de l'intelligence artificielle au sein de la DRSD ?

Général de corps d'armée Philippe Susnjara. Nous investissons déjà le champ informationnel ; comme dans le domaine cyber, nous partageons la tâche avec le Comcyber : celui-ci s'occupe du ministère des armées et nous nous focalisons sur la BITD. Service de renseignement, nous nous inscrivons dans la contre-ingérence informationnelle pour voir dans quelle mesure certains acteurs peuvent attaquer la réputation d'une entreprise et divulguer de fausses informations, par exemple pour l'empêcher d'obtenir un marché. Une petite cellule suit ces dossiers, notre objectif étant, dans l'année qui vient, de nous brancher sur ceux, dans la sphère institutionnelle ou industrielle, qui mènent déjà des actions très intéressantes ; les grands groupes font déjà de la veille informationnelle, mais pas forcément dans leur chaîne logistique. Comme pour le cyber, il peut y avoir des attaques contre les petites entreprises, qui sont des maillons de cette chaîne, pour contourner la protection que déploient les grandes sociétés. Nous essayons d'effectuer une veille générale tout en nous focalisant sur quelques thématiques, par exemple celle des marchés d'exportation vitaux pour certaines entreprises. Ensuite, il faut être capable de faire remonter l'information vers les acteurs qui peuvent agir.

Quand j'ai pris mon poste, j'ai créé une cellule de prospective et d'anticipation : nous utilisons déjà l'intelligence artificielle dans nos propres outils, mais nous devons nous demander ce que cette révolution nous apportera. Nous menons des réflexions sur le métavers : quelles sont ses implications pour nous ? Que signifie le fait de pouvoir vivre dans un monde parallèle ? Nos

agents devront-ils disposer d'avatars pour agir dans ce champ ? Devons-nous être officiellement présents dans le métavers ? Doit-il y avoir une DRSD officielle dans le métavers ? Nous sommes encore dans le domaine de la science-fiction car les définitions sont complexes. Il nous faut mener des études prospectives dans ce domaine. Nous suivons ces sujets. La priorité à mes yeux est d'utiliser tous les outils pour tirer le maximum de nos bases de données et de suivre en parallèle les évolutions technologiques pour ne pas être distancés, le problème étant leur coût élevé. Les voitures électriques de type Tesla, qui communiquent et filment en permanence leur position, diffèrent fortement des véhicules classiques : il en va de même dans tous les domaines de la vie.

Mme Mélanie Thomin (SOC). Je vous remercie pour votre présentation reliée au triptyque « connaissance, compréhension, anticipation » de la RNS. La fonction de contre-ingérence de la DRSD est amenée à se renforcer ; cette logique paraît cohérente à la lumière de la dégradation du contexte stratégique général et de l'intensification des compétitions sectorielles. Vous avez évoqué les crédits alloués au renseignement, plus particulièrement ceux destinés à votre direction. Vous avez également défini certaines priorités de renforcement, notamment dans le domaine du cyber. Pouvez-vous nous préciser vos autres priorités de renforcement, même si vous avez déjà eu l'occasion de citer quelques secteurs dans lesquels vous êtes en pointe ?

Quel sera le rôle de la direction dans le contrôle des trajectoires des anciens militaires ? Quels sont, compte tenu de l'expérience de la DRSD, les enjeux de ce contrôle nouveau ?

Général de corps d'armée Philippe Susnjara. Nous exerçons déjà un contrôle sur la trajectoire des anciens militaires, mais l'article 20 de la LPM nous fournira un moyen d'action supplémentaire avec l'outil d'entrave. En outre, les anciens militaires devront faire une déclaration s'ils veulent travailler pour des entreprises ou au profit d'États étrangers. Nous devons en revanche nous montrer flexibles sur le type d'emplois que l'on qualifie de sensibles, cette catégorie pouvant évoluer rapidement et varier selon les pays. Tout le monde parle des pilotes de chasse, qui pourraient divulguer des savoir-faire, ces révélations pouvant avoir des implications en cas de confrontation. On peut imaginer d'autres emplois sensibles dans les armées, par exemple ceux liés à la dissuasion où l'on acquiert des connaissances techniques et des savoir-faire éventuellement transférables : là aussi, notre attention peut différer en fonction des États : tout intéresse la Chine, mais d'autres États ne peuvent être motivés que par certains aspects répondant à un besoin spécifique de montée en puissance. Nous devons nous adapter à l'évolution des centres d'intérêt de nos compétiteurs. Le mécanisme de l'article 20 sera en tout cas très utile.

En interne, je souhaite accomplir un effort énorme sur les ressources humaines. Mes prédécesseurs ont lancé plusieurs grands projets que je veux poursuivre pour les mener à leur terme, parfois en les améliorant. Nous devons prolonger la dynamique de transformation de la direction lancée ces dernières années. Nous tenons également à développer des outils permettant à nos agents d'apporter une plus-value supplémentaire et d'être davantage formés. À ce titre, je souhaite mettre en avant un centre de formation, qui sera assez modeste mais qui améliorera nos échanges avec nos partenaires du premier cercle – je souscris ainsi complètement aux recommandations de la CNRLT – et qui valorisera nos formations pour mieux les inscrire, notamment par des certifications, dans des parcours de carrière. L'objectif

est de fournir des formations répondant au juste besoin tout au long de la carrière, là aussi pour suivre les adaptations des fonctions.

De mon point de vue, il n'est plus possible de séparer la protection physique de la protection cyber : les deux sont liées. Historiquement, la DRSD s'est plutôt concentrée sur la protection physique, puis elle est venue au cyber, alors que les jeunes entreprises viennent à s'intéresser à la protection physique par le cyber : après avoir mis un antivirus, elles s'aperçoivent de l'utilité de mettre un verrou sur la porte du bureau, alors que notre direction a accompli le chemin inverse. Les deux protections sont liées, donc les inspecteurs de la DRSD sur le terrain doivent, sans être des experts, maîtriser un minimum de connaissances cyber ; ce bagage minimal doit leur permettre de s'adresser à des experts en cas de doute ou de problème pour obtenir le bon conseil ou la bonne information : nous sommes en train de concrétiser cette exigence, notamment dans le cadre du centre d'alerte et de réaction aux attaques informatiques – Cert pour Computer Emergency Response Team – ; nous travaillons également à maîtriser l'extraterritorialité des lois et des normes, car sans être infaillibles dans tous les domaines, nos agents doivent avoir des connaissances de base leur permettant d'identifier un problème et de se retourner vers les experts de la question.

M. Jean-Charles Larsonneur (HOR). Je vous remercie beaucoup de votre éclairage sur ce projet de LPM, auquel je suis particulièrement attentif en tant que rapporteur du programme 144 Environnement et prospective de la politique de défense de la loi de finances.

Je ne peux que soutenir vos priorités – formation, Cert, cyber, y compris dans les milieux virtuels. Les bâtiments et les infrastructures sont, plus que d'autres domaines, sensibles à l'inflation : est-ce une préoccupation pour vous ?

L'actualité est marquée par les fuites de documents du Pentagone, qui pourraient constituer une hypothèse de travail pour la DRSD. Comme vous l'avez dit, il faut se montrer très prudent car les rares détails sur la source présumée, « OG », peignent le tableau d'une extrême droite américaine, qui demeure, comme en France, la principale menace en matière de radicalisation et de terrorisme endémique. Comment la DRSD se prépare-t-elle à gérer d'éventuelles fuites de ce genre en France ?

Général de corps d'armée Philippe Susnjara. Nous sommes attentifs à l'inflation mais nous sommes assez confiants car la majorité des engagements ont été réalisés et il ne nous reste qu'une petite part cette année, peu élevée par rapport au coût global du fort de Vanves. Les autres projets de la direction sont financés, et nous avons des assurances pour deux des trois chantiers en province. Le vrai sujet est qu'au-delà du nouveau bâtiment, essentiel pour nous, nous devons mener une réorganisation spatiale car certains bâtiments du fort sont assez anciens ; nous verrons, au cours de la LPM, si nous pouvons faire évoluer cette infrastructure, mais il est trop tôt pour se prononcer. Je vois ce que je voudrais, mais nous ferons avec les moyens mis à notre disposition.

Les fuites se trouvent au cœur du métier de contre-ingérence, dans son volet centré sur les compromissions. Nos actions dans ce domaine sont multiples. Tout d'abord, il y a les habilitations : qui a accès à nos informations ? Il faut s'assurer que seules les personnes habilitées ont accès à des informations sensibles ; les personnes qui n'ont pas besoin de les

connaître ou qui ne sont pas fiables ne doivent pas y avoir accès. Ensuite, nous déployons une protection physique et cyber conforme à la réglementation des données : sont-elles bien enregistrées ? Sont-elles bien stockées ? Leur circulation est-elle bien encadrée ? Les inspecteurs et le centre d'expertise effectuent tous ces contrôles. Dans ce domaine, encore moins que dans les autres, le risque zéro n'existe pas ; quelqu'un de bonne volonté qui se fait voler son ordinateur portable après avoir oublié de chiffrer son disque dur peut nous exposer à des fuites – c'est comme si quelqu'un mettait des barreaux aux fenêtres mais ne fermait pas sa porte. Le risque principal de fuites ne tient pas à la malveillance mais à l'erreur humaine. Porter une grande attention à ce risque est notre lot quotidien ; pour le déjouer, il faut beaucoup de sensibilisation, de conseil et, de temps en temps, quelques remontrances.

M. Christophe Blanchet (Dem). Vous pouvez enquêter sur les réservistes RO1 et RO2, mais comment ferez-vous avec le doublement de cette population que prévoit la LPM ? Quel regard portez-vous sur la réserve citoyenne, qui doit augmenter dans de nombreux ministères et dans la cyberdéfense ? Effectuerez-vous les mêmes investigations pour ces réservistes citoyens, qui n'auront pas les mêmes compétences mais qui aspireront à pleinement s'engager en faveur des armées ?

Lors de la mission d'information sur les réserves que nous avons menée il y a deux ans avec mon ancien collègue Jean-François Parigi, nous avions été surpris qu'aucune disposition légale n'oblige un militaire, donc un réserviste, à informer sa hiérarchie en cas de condamnation pénale. Certes, vous enquêtez au moment de l'entrée d'une personne dans l'armée, mais une fois entré, le militaire ou le réserviste n'est soumis à aucune obligation de déclaration. Travaillez-vous sur ce thème ? Nous avons des retours sur des personnes condamnées qui prospectaient sur des éléments qui avaient entraîné leur condamnation – je pourrais vous fournir des exemples concrets en aparté. Que faire contre les possibles ingérences nées de captures d'écran ou de vidéos compromettantes de personnes, qui n'ont pas commis de délit mais qui ont honte de ces images et qui subissent un chantage ?

Général de corps d'armée Philippe Susnjara. Le doublement des effectifs de la réserve opérationnelle constitue en effet un vrai défi. Nous devrons améliorer le processus d'habilitation, notamment en automatisant certaines étapes. Pour la réserve citoyenne, il n'y a pas de saisine systématique, on nous demande de temps en temps ce que l'on pense d'un individu. Nous sommes devant un vrai défi avec le doublement des réserves opérationnelles, mais nous le relèverons ; il faut dire aussi que la profondeur de l'enquête dépend évidemment du poste auquel est affecté le réserviste.

Nous consultons les fichiers du ministère de l'intérieur, mais la déclaration de condamnation n'est en effet pas systématique pour les personnes déjà dans les cadres – une obligation de déclaration n'offrirait néanmoins pas de garantie totale. Nous avons de bons contacts, à l'échelle locale, avec les commissariats et les gendarmeries : les informations remontent souvent, et nous vérifions ce qu'il en est. Pour les personnes habilitées, nous allons rarement au bout du délai de renouvellement de cinq ou sept ans, en fonction du degré très secret ou secret, parce que l'habilitation est liée à la fonction et non à la personne en France – j'ai changé trois fois de poste en cinq ans, j'ai donc fait trois demandes d'habilitation. Nous vérifions donc assez régulièrement les casiers judiciaires des agents.

M. le président Thomas Gassilloud. Nous vous remercions de nous avoir éclairés sur la DRSD et nous vous souhaitons bon courage pour la suite de vos missions et pour les quelques centaines de milliers de demandes que vous avez à traiter chaque année.