ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
3 juin 2026
Séance de 9 heures

Compte rendu n° 72

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

– Audition, à huis clos, du général de corps d'armée Aymeric Bonnemaison, directeur du renseignement et de la sécurité de la défense (DRSD) et de Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI) (cycle « Guerre hybride et continuum de conflictualités »)..... 2

Présidence de M. Loïc Kervran,
Vice-président

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

M. Loïc Kervran, président. Avant toute chose, je vous prie d'excuser l'absence du président Jean-Michel Jacques, qui conduit cette semaine une délégation de notre commission au Vietnam.

Dans le cadre du cycle d'auditions consacré à la guerre hybride et au continuum de conflictualités, nous accueillons M. le général de corps d'armée Aymeric Bonnemaison, directeur du renseignement et de la sécurité de la défense (DRSD), et Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI).

C'est la première fois que nous entendons conjointement deux directeurs de services de renseignement parmi les six dits du « premier cercle ». Ces deux services, qui dépendent respectivement du ministère des armées et du ministère de l'intérieur, sont des acteurs clés dans l'anticipation et la prévention des menaces hybrides sur notre territoire national, notamment en matière de contre-ingérence et de contre-espionnage.

Les ingérences étrangères sont au cœur des actions hybrides menées par nos compétiteurs. Elles constituent l'un des exemples de rétroactions déstabilisatrices que ces derniers pourraient mener sur le territoire national en parallèle d'un conflit majeur dans le cœur de l'Europe, ainsi que le prévoit le scénario central de la nouvelle revue nationale stratégique (RNS).

La contre-ingérence vise à déceler les intentions adverses en identifiant et en neutralisant toute menace pouvant conduire à des actes hostiles de la part d'organisations, de groupes ou d'individus isolés. Pour surveiller et contrer les dispositifs d'espionnage, la DGSI et la DRSD engagent des actions préventives et sensibilisent les acteurs visés par des tentatives d'ingérence et de pillage de leurs ressources.

Madame la directrice générale, mon général, nous attendons de vous un panorama des menaces hybrides auxquelles sont confrontés vos services. Vous nous préciserez comment ces derniers s'efforcent d'y répondre, les moyens dont ils disposent et les éventuelles limites des dispositifs que vous déployez pour prévenir ces menaces.

Mme Céline Berthon, directrice générale de la sécurité intérieure. Je suis honorée et ravie d'intervenir aux côtés du général Bonnemaison, puisque nous œuvrons au quotidien sur le territoire national dans nos champs respectifs de compétences, qui ne se chevauchent pas mais s'accolent – la DGSI couvrant la sphère civile et la DRSD la sphère militaire.

La DGSI, service intérieur en charge de la lutte contre le terrorisme, les ingérences et l'espionnage, doit d'ores et déjà affronter une menace à 360 degrés qui nous permet de toucher du doigt un terreau de menaces important, persistant et se diversifiant.

Tout d'abord, nous sommes toujours confrontés à une menace transnationale de nature terroriste dirigée contre notre territoire, sous un format différent de ce que notre pays a connu ces dix dernières années – singulièrement au milieu des années 2010, au moment de la vague la plus forte. La menace terroriste islamiste est toujours élevée, et protéiforme. Dans un monde de radicalités et de conflictualités, nous devons aussi prendre en compte l'amplification

d'une menace de nature terroriste qui peut relever d'autres types d'extrémismes, en particulier de mouvances dites « ultra ».

Nous faisons également face, depuis plusieurs années, à une intensification des ingérences étrangères, qui trouvent à se déployer sur notre territoire en raison d'un contexte international dégradé qui alimente les velléités de certains pays de se mêler de nos affaires intérieures. Pour rester pudique à ce stade, je citerai deux pays qui se sont distingués dans ce schéma de compétition internationale en faisant preuve d'agressivité sur notre territoire : la Russie et l'Iran. La menace prend la forme d'ingérences institutionnelles et d'espionnage, d'ingérences économiques, d'actions terroristes et de sabotage, de cyberattaques ou encore de manipulations de l'information.

Le niveau de ces menaces soulève des enjeux de capacité opérationnelle pour nos services : il nous appartient de nous préparer à une montée en puissance pour empêcher une logique d'asphyxie.

Dans ce contexte, la notion d'hybridité est un sujet pris en compte et identifié clairement, notamment dans l'exercice de la revue nationale stratégique. Publiée le 14 juillet 2025, cette dernière actualise un diagnostic préalablement établi en 2022 et nous demande de nous préparer à l'hypothèse d'un engagement massif des armées dans un conflit de haute intensité en Europe, ainsi qu'à un déferlement d'attaques hybrides sur le territoire national.

Nous identifions quatre dynamiques structurantes : l'hypothèse du durcissement de la posture russe – l'actualité, encore ce matin, nous conduit à nous projeter en ce sens ; le resserrement stratégique entre des pays que nous pouvons qualifier de compétiteurs – la Russie, la Chine, l'Iran, ou encore la Corée du Nord ; les incertitudes sur la pérennité de la solidarité transatlantique, par contraste avec les logiques de solidarité qui ont pu dominer par le passé ; enfin, la persistance de menaces transnationales – terrorisme, narcotrafic, cybercriminalité.

Nous nous inscrivons dans la doctrine établie par le secrétariat général de la défense et de la sécurité nationale (SGDSN), qui nous demande de nous préparer, dans une optique interministérielle, à lutter contre les stratégies hybrides.

Vous connaissez les critères clés de l'hybridité. Il s'agit d'une logique de stratégie globale, conçue et conduite par un acteur hostile avec un haut niveau d'intégration aux échelons politiques et stratégiques, avec des modes d'action qui mêlent civil et militaire – ce qui donne beaucoup de sens à notre audition commune – et qui peuvent passer par le renseignement et l'influence. Point important, elle utilise une combinaison intégrée et volontairement ambiguë d'actions – l'ambiguïté étant confortable, soit pour plaider le déni plausible, soit pour complexifier l'imputation d'une action.

Ces actions visent à obtenir des gains, en évitant d'entrer directement dans un conflit armé et en gérant la logique d'escalade, soit par intimidation, soit par déstabilisation de l'adversaire.

Le concept n'est pas nouveau pour nous : même si nous n'utilisions pas ce mot-là, nous étions déjà engagés de fait dans le traitement de ces menaces qui font partie de notre champ de compétence naturel, en tant que menant ou concourant – notamment aux côtés de la DRSD.

La DGSI est totalement impliquée dans la préparation de l'État et de la nation à la réalisation de ces menaces dans le cadre du plan de défense et de sécurité nationale (PDSN), qui nous demande de proposer des mesures de cadencement de la montée en puissance de l'État à l'intérieur de ce scénario central de la RNS.

Pour nous, ce travail soulève trois enjeux : capacitaire, légal et organisationnel. Il nous engage également à renforcer nos liens avec la sphère défense, comme dans le cadre de l'exercice interministériel Orion 2026, qui nous a permis d'identifier les enjeux et de constater l'importance d'un partage encore accru des renseignements. Le renforcement du dialogue entre les ministères de l'intérieur et de la défense s'est aussi traduit, au début de l'année 2026, par la signature d'une nouvelle directive de coopération civilo-militaire et par des travaux d'actualisation de la défense opérationnelle du territoire, avec ses mesures non permanentes. Il se manifeste enfin dans les réflexions conduites au sein de la communauté des services de renseignement – la coordination nationale du renseignement et de la lutte contre le terrorisme, notamment, conduit elle aussi des travaux de déclinaison du PDSN.

J'aimerais conclure sur un point d'attention : en temps de crise, il faudra s'appuyer sur des organisations déjà éprouvées et qui ont démontré leur solidité. Le respect des chefs de file et du principe menant-concourant me paraît absolument fondamental : dans un contexte de crise, il nous faudra non pas réinventer, mais consolider les organisations. Ce que nous menons au niveau national, dans les instances centrales, devra aussi pouvoir être décliné à l'échelon territorial en respectant ce schéma d'organisation. Nous ne serons solides que si nous nous appuyons sur des savoir-faire qui ont déjà été éprouvés et sur lesquels nos équipes sont solidement arrimées.

M. le général de corps d'armée Aymeric Bonnemaison, directeur du renseignement et de la sécurité de la défense. La guerre hybride est un sujet sur lequel nous travaillons déjà quotidiennement et de manière conjointe avec la DGSI, tant au niveau des directions centrales que des régions.

Dans une guerre hybride, pour faire court, l'adversaire cherche à nous soumettre, sans nécessairement nous combattre – au sens militaire du terme. Il s'agit de l'hybridation de capacités militaires ou non, directes ou indirectes, qui vise essentiellement à nous contraindre et à nous affaiblir. Cela cible tous les champs de la société : le politique, dont vous êtes les représentants, l'économique et le social. Cela mobilise des moyens d'actions dont les plus nouveaux et les plus récurrents sont les cyberattaques, la manipulation de l'information et l'instrumentalisation du droit et de l'économie. Et cela passe de plus en plus par des *proxies,* c'est-à-dire par des intermédiaires qui complexifient un peu l'attribution des actions.

Vis-à-vis des démocraties occidentales, dont le territoire est moins susceptible de subir des attaques terrestres directes, cette forme de guerre peut être redoutablement efficace si le pays en question n'est pas préparé, c'est-à-dire en mesure de détecter, d'identifier, d'entraver et d'anticiper, et s'il ne fait pas d'efforts de sensibilisation réguliers.

Nous avons la chance de pouvoir nous appuyer sur la revue nationale stratégique publiée en juillet dernier, qui place l'hybridité au cœur des objectifs stratégiques – tous sont concernés, et le neuvième objectif en particulier fait de cette dernière une cible de la contre-ingérence de défense élargie, donc de l'action de la DRSD. Le scénario principal identifié est celui d'un engagement majeur hors du territoire national, qui s'accompagnerait simultanément

d'une hausse massive des attaques hybrides sur notre sol. La DRSD participe aux travaux pilotés par le SGDSN afin d'élaborer une réponse structurée à ce scénario – je sais que le préfet Xavier Brunetière a déjà abordé ce point devant vous. Elle a également participé activement à l'exercice Orion 2026, notamment à son volet 3 qui portait sur les répercussions de ce scénario sur le territoire national – la coopération avec la DGSI a d'ailleurs été très étroite dans le cadre de cet exercice.

Les actions hybrides peuvent viser tout autant les forces armées, en France et à l'étranger, que la sphère défense élargie. Très concrètement, pour évoquer des événements rendus publics, il peut s'agir du survol d'emprises militaires par des drones, ou encore de campagnes de désinformation comme celle qui évoquait la présence de cercueils sous la tour Eiffel. Ce sont là des exemples d'actions hybrides que vous avez déjà identifiées.

Compte tenu de leur nature, ces stratégies hybrides rendent plus complexe l'identification des menaces qu'elles représentent pour l'ensemble des institutions et des organisations publiques et privées, militaires et civiles. Par conséquent, elles rendent difficile la mise en place rapide de mesures de protection adaptées.

En tant que service de contre-ingérence dans la sphère défense élargie, la DRSD est en première ligne dans la lutte contre ces menaces. Elle assure la protection de 270 000 ressortissants de défense du ministère des armées, de l'ensemble de ses emprises – en métropole, outre-mer et à l'étranger, dans le cadre des opérations extérieures – ainsi que de 4 000 entreprises de la base industrielle et technologique de défense (BITD) – un chiffre qui a tendance à s'accroître. La partie visible de la mission de la DRSD se trouve dans les enquêtes administratives – plus d'un demi-million l'année dernière – et dans les inspections physiques et cyber – plus de 250 pour les premières, un peu moins d'une cinquantaine pour les secondes. Mais le service lutte aussi contre les ingérences par le renseignement et l'identification des menaces.

Face à la guerre hybride, l'action de la DRSD repose sur deux piliers : l'identification des menaces, c'est-à-dire la mission pure de renseignement, et la détection de nos propres vulnérabilités – c'est le pilier protection, qui recouvre nos actions d'audit, d'accompagnement et d'inspection. Cette articulation doit permettre à la sphère défense d'être plus résiliente face à toutes les menaces que j'ai mentionnées.

Face à l'hybridité, trois axes d'efforts ont été développés ces dernières années : l'espace cyber, les prédations économiques, et la protection physique « nouvelle génération ».

En matière de cyberdéfense d'abord, la DRSD détient des capacités en propre pour prévenir les attaques cybernétiques qui affectent les réseaux classifiés de la défense et, de plus en plus souvent, les entités de l'industrie de défense. Le service contribue à l'identification des menaces dans le domaine cybernétique, avec le commandement de la cyberdéfense (Comcyber) pour le ministère des armées et l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour les opérateurs d'importance vitale.

Les attaques sont en augmentation croissante. Elles sont d'origine criminelle ou proviennent de services de renseignement (SR) étrangers qui cherchent à pénétrer nos systèmes ou à les perturber – l'interaction entre cybercriminalité et SR étrangers est bien sûr une combinaison permanente. Ces groupes ont cherché à porter atteinte, par exemple, aux sites internet institutionnels des sociétés françaises impliquées dans la fourniture d'armes en Ukraine

– en particulier d'armement terrestre – en recourant notamment à des dénis de service, un outil peu sophistiqué mais qui entrave l'entreprise et peut entamer sa réputation à l'export.

Selon notre bilan de l'année 2025, publié récemment, 13% des faits de sécurité relèvent d'attaques purement cyber, dont 25% conduisent essentiellement à des exfiltrations de données. De ce fait, la DRSD a développé depuis deux ans une capacité spécifique visant à renforcer la cybersécurité des très petites, petites et moyennes entreprises (TPE-PME) de défense au travers d'un centre d'alerte et de réaction aux attaques informatiques des entreprises de défense (CERT [ED]). Nous avons ciblé ce segment car il était le plus désarmé en matière de cybersécurité. En cyber, l'attaquant ciblera en priorité le maillon faible pour ensuite remonter vers des cibles mieux protégées.

Le CERT principal en France est celui de l'Anssi (CERT-FR) ; le Comcyber en a également un pour les armées (CERT-MIL). Le CERT [ED] permet aux entreprises abonnées – plus de 550 aujourd'hui – de disposer d'un référent pour les aider à améliorer leur cybersécurité et les accompagner en cas d'attaque avérée. À travers le CERT [ED], nous pouvons les conseiller, leur signaler leurs failles de sécurité, voire réaliser des tests un peu plus poussés sur leurs vulnérabilités.

Deuxième volet d'efforts : la lutte contre les manœuvres de prédation et de déstabilisation économique. Dans sa mission de protection de la sphère défense élargie, la DRSD attache une grande importance à la surveillance des initiatives étrangères visant les entreprises de la BITD. Nous sommes attentifs aux grands systémiers, mais aussi à toutes les entreprises de la chaîne de production et d'approvisionnement, y compris les TPE, avec une attention particulière à l'égard des entreprises duales.

Dans le cas de ces dernières, nous nous coordonnons avec la DGSI en fonction de l'importance des sujets militaires ou civils afin de nous assurer que nous couvrons tout le spectre, et lorsque nous convergeons sur une entreprise à défendre, nous suivons un système de menant-concourant – très concrètement, nous nous répartissons les visites d'audit. La DRSD s'appuie pour cela sur son maillage territorial et de contacts de terrain. Ses agents, présents au plus près des entreprises, apportent un conseil en matière de protection, mais permettent aussi de détecter les signaux faibles. Les structures locales de la DRSD travaillent sur ces sujets de concert avec tous les partenaires institutionnels des territoires – la DGSI, les autorités préfectorales, la direction nationale du renseignement territorial et tous les acteurs en région.

Nous travaillons à prévenir les ingérences capitalistiques. L'idée est d'éviter que des investissements trop importants de la part d'un acteur économique étranger lui donnent accès aux technologies et aux savoir-faire des entreprises œuvrant pour la défense, ou lui confèrent suffisamment de pouvoir pour orienter leur stratégie à l'encontre des intérêts français.

En matière économique et technologique, certains pays font également un usage très décomplexé du droit, avec des dispositions à portée extraterritoriale – ce qu'on appelle la *lawfare*, la guerre juridique, ou encore l'arsenalisation du droit, autrement dit l'utilisation de dispositifs juridiques à des fins stratégiques. Cette forme d'ingérence permet à ces États de contraindre l'activité des industriels français, soit en limitant leurs capacités d'approvisionnement, soit en les empêchant de commercialiser leurs produits.

Sur ces sujets, la DRSD amplifie son travail d'anticipation stratégique pour alerter les entreprises concernées par les menaces et les accompagne pour sécuriser au plus tôt leurs projets de développement. À l'heure actuelle, nous nous concentrons particulièrement sur nos jeunes pousses dans le domaine de l'intelligence artificielle (IA) et du quantique – avec la DGSI lorsqu'elles sont duales, ce qui est le cas de beaucoup d'entre elles.

Le troisième volet d'efforts concerne la protection des emprises et la lutte contre les atteintes aux biens de la sphère défense, qui, comme les personnes, sont au cœur de nos missions. Nous observons notamment des détériorations et des vols de matériel sensible. Cela peut paraître anodin, mais le caractère répétitif et parfois coordonné de ces actions peut nous mettre sous tension et fragiliser les systèmes de défense. Nous avons observé ces derniers mois des actions de plus grande ampleur liées à des survols de sites sensibles, largement relayées par la presse, et constaté un doublement des vols au-dessus des zones de l'industrie de défense et militaire en 2025.

La DRSD, en lien avec la direction de la protection des installations, moyens et activités de la défense (DPID) et avec la direction générale de l'armement (DGA), concourt à l'effort de sécurisation des biens. Nous menons ainsi tout au long de l'année des inspections au service des emprises du ministère des armées et des entreprises de la BITD, afin de nous assurer que leur niveau de sécurité est adapté à la sensibilité des lieux. Pour accompagner au mieux les acteurs, nous augmentons notre capacité d'inspection, notamment grâce à l'automatisation de certains processus – nous avons quasiment quadruplé le nombre d'inspections en dix ans.

À ces trois efforts principaux, je pourrais ajouter ceux que nous menons pour faire face aux campagnes de désinformation, habituer les entreprises à les détecter et à les analyser, et les sensibiliser à cette menace et aux incidences possibles sur leurs exportations, leur production ou leur réputation.

Au cœur de notre mission se trouve la sensibilisation. La DRSD effectue ses actions de sensibilisation partout en France, avec près de 46 000 personnes sensibilisées en 2025. Le service s'adapte à tous les publics qu'il rencontre – forces armées ou BITD – en variant notamment les supports. Nous publions une lettre d'information économique sur les réseaux : celle qui vient de sortir accompagne la tenue du Salon mondial de la défense et de la sécurité Eurosatory, tandis que la précédente, peut-être un mois auparavant, faisait le bilan de l'année 2025. Nous communiquons et publions aussi des guides à destination des entreprises, par exemple pour les aider à accompagner une visite étrangère. Il s'agit de recommandations simples et de bon sens, mais assez exhaustives. En 2025, la DRSD a également organisé un séminaire dédié aux référents sécurité des pôles de compétitivité et clusters de défense, qui a permis d'alerter largement sur les menaces et les enjeux de bonnes pratiques. Ces dernières années, la DRSD insiste également sur le domaine de la recherche en lien avec la défense.

La mission de sensibilisation est particulièrement importante dans ce contexte de guerre hybride. Il faut considérer aujourd'hui qu'un citoyen ou un militaire averti est déjà un premier rempart face aux menaces hybrides – c'est d'ailleurs l'une des actions identifiées dans la RNS.

Initialement, les actions de la DRSD portaient sur l'humain – enquêtes administratives, accompagnement des fragilités individuelles – et sur la protection physique des emprises. Depuis dix ans, nous avons dû évoluer dans la protection cyber, réputationnelle,

capitalistique et juridique, et même dans le conseil sur les approvisionnements. La conjugaison des acteurs et des modes d'action diverge en fonction des pays agresseurs : à titre d'illustration, les Russes ont des compétences avérées dans le cyber, le réputationnel et l'humain ; les Chinois recourent massivement à la *lawfare* et au cyber ; les Américains, quant à eux, sont particulièrement actifs dans le capitalistique et la *lawfare*.

Le domaine de l'hybridité est extrêmement vaste. Le défi de notre service est donc d'éviter la dispersion. Pour ce faire, nous priorisons de grands axes d'effort – la dissuasion nucléaire, les rétroactions sur le territoire national, la montée en puissance d'une économie de guerre et de ses capacités de production – et concentrons nos actions sur des cibles prioritaires. Dans ces domaines, nous réalisons du *red teaming*, c'est-à-dire que nous nous mettons à la place d'un adversaire et imaginons des scénarios d'attaque, après quoi nous focalisons nos audits et nos inspections sur les points de faiblesse potentiels que cela peut avoir fait apparaître.

La DRSD va ainsi à la chasse aux menaces et poursuit en parallèle le recueil de toutes les compromissions qui lui sont signalées, afin de repérer la cohérence et la coordination qui pourraient se dessiner derrière.

M. Loïc Kervran, président. Nous en venons aux interventions des orateurs des groupes.

M. José Gonzalez (RN). Au nom du groupe Rassemblement national, je salue l'engagement de vos services et de leurs personnels en faveur de la protection de notre souveraineté, dans un contexte de durcissement des menaces qui vous met chaque jour à l'épreuve.

Les publications récentes de la DRSD et de la DGSI montrent une évolution extrêmement préoccupante des stratégies d'ingérence visant notre BITD. La DRSD alerte sur la multiplication des cyberattaques, par ricochet, contre les sous-traitants de la défense, sur les tentatives de sabotage ou de paralysie industrielle, mais aussi sur les opérations de captation technologique ciblant les PME stratégiques françaises. Dans le même temps, la DGSI souligne un changement de nature de ces actions, qui ne relèvent plus seulement de l'espionnage classique mais s'inscrivent désormais dans des stratégies globales mêlant influence économique, infiltration numérique, manipulation informationnelle et dépendance technologique.

À ce titre, la publication par la DRSD d'une alerte spécifique en amont du salon Eurosatory 2026 est particulièrement révélatrice. Les grands événements internationaux de défense apparaissent comme des espaces privilégiés de captation d'informations sensibles, de ciblage humain et d'intrusion numérique.

Considérez-vous que notre BITD est suffisamment protégée par notre cadre juridique face aux stratégies hybrides déployées par certaines puissances étrangères contre la France ? Quels sont selon vous les points d'amélioration prioritaires à court terme ?

Par ailleurs, comment vos services appréhendent-ils désormais les grands salons internationaux comme Eurosatory, véritables zones de confrontation informationnelle et technologique ? Où en est-on dans la contre-ingérence concernant ces événements et dans la sensibilisation des industriels français ?

M. le général de corps d'armée Aymeric Bonnemaison. On ne sera jamais assez protégé face aux menaces hybrides. Il nous faut donc être toujours en éveil et diffuser cet esprit de vigilance au sein de l'État. Il ne faut pas croire que cette menace est surjouée : elle existe bel et bien.

S'agissant d'Eurosatory, nous sommes déjà très impliqués. À l'occasion de nos opérations de sensibilisation des entreprises et plus particulièrement des exposants, nous constatons que nous avons affaire à des gens de plus en plus avertis, qui nous écoutent et appliquent les mesures parfois simples que nous leur indiquons. Nous sommes en contact avec eux en amont et pendant le salon, où nous sommes très présents. Dans le guide que nous distribuons ou encore dans notre lettre d'information dédiée à Eurosatory figure notamment un numéro vert qui permet de nous alerter sur des comportements atypiques lors des visites – faux journalistes, photos ou questions un peu trop poussées.

La difficulté d'Eurosatory cette année tient pour nous à son succès, qui étend encore le spectre des protections à mettre en place. Dans le domaine technologique, nous sommes de plus en plus impliqués dans la DefTech, cette technologie de défense souvent duale et composée de nouveaux acteurs. L'avantage est que nous sommes en contact avec ces derniers dès leur création : les fondamentaux sont donc déjà posés et, sur ces sujets en particulier, la jeune génération n'est pas naïve.

Mme Céline Berthon. Dans ce domaine fondamentalement militaire, la DGSI intervient en tant que concourant. Nous devons être capables d'accepter la menace et d'y adapter nos outils, de la même façon que nous nous sommes dotés d'outils antiterroristes – de protection de notre territoire, ou encore d'entrave – qui nous ont permis de maîtriser davantage la menace, à défaut de la faire reculer totalement.

Il ne s'agit pas de décliner ce sujet dans l'ensemble de nos champs, mais d'accepter que la menace ne soit plus seulement terroriste, mais aussi d'ingérence. Dans ce cadre, l'enjeu est de qualifier la menace – je pense que c'est bien réalisé –, de sensibiliser, afin d'être capable de détecter et d'intervenir le plus en amont possible, et enfin d'accepter les modalités de protection.

Ainsi, certains individus ne sont plus les bienvenus sur certains salons car ils sont porteurs d'un risque non pas de violence, mais de prédation et de captation : il est donc légitime de les maintenir à distance. Cela peut passer par des mesures de criblage ou d'empêchement d'accès au territoire national, de manière à étanchéifier l'accès au cœur de notre réseau. Nous pouvons dès lors concentrer nos moyens humains, techniques et de renseignement sur le cœur des porteurs de menaces plutôt que de nous disperser dans la surveillance d'individus qu'on peut maintenir à distance.

C'est notre philosophie : sensibiliser au plus tôt, protéger au maximum et assumer de maintenir nos adversaires à distance.

M. Yannick Chenevard (EPR). En quelques années, nous avons vu s'ajouter aux actions d'espionnage classique les cyberattaques isolées qui font que nous sommes pris aujourd'hui dans une forme de continuum : une action numérique peut préparer une action physique, et une action physique, même modeste, peut avoir des effets informationnels ou politiques importants. Nous avons longtemps raisonné par catégories – terrorisme, cyber,

influence – mais il semble que les frontières s'effacent désormais pour céder la place à une zone beaucoup plus grise.

Comment les services de la DGSI font-ils le tri entre un incident, un test préparatoire et une opération structurée ?

Notre BITD est en train de monter en puissance, ce qui conduit à modifier la taille des emprises d'un certain nombre de nos usines. La DRSD a-t-elle perçu des tentatives d'approche indirectes – sans que les acteurs en aient nécessairement conscience d'ailleurs –, soit de la part des services qui instruisent les dossiers d'urbanisme, soit de la part d'associations qui pourraient être manipulées en vue de ralentir le déroulé des opérations ?

Mme Céline Berthon. Depuis quelque temps déjà, avant même d'employer le terme de guerre hybride, nous observions la superposition des modes opératoires et des actions. Le défi, dans ce contexte, est de savoir à qui et à quoi nous avons affaire, et quels sont les objectifs de la manœuvre.

La notion d'espionnage est définie depuis longtemps : c'est l'accès à une information non publique – et pas seulement estampillée « secrète ». Vos travaux parlementaires et votre activité politique, lorsqu'ils ne sont pas publics, peuvent ainsi être une cible d'espionnage et l'on peut tenter d'accéder au contenu de vos échanges, soit en vous approchant ainsi que vos collaborateurs, soit par le biais de cyberattaques ciblant vos moyens de communication de manière à capter ce qui se dit en interne. L'espionnage est traditionnellement le fait d'espions, c'est-à-dire de salariés de pays étrangers – ce sont des fonctionnaires d'État, employés par des services de renseignement et dont la mission première est de chercher ces informations non publiques.

On a vu ce champ s'étendre vers des actions d'ingérence, qui visent à se mêler des affaires intérieures d'un pays. Il ne s'agit ni de diplomatie ni d'influence, mais d'une logique d'actions hostiles et bien souvent dissimulées. Il s'agit de nous faire tort, mais sans avoir le drapeau accroché aux épaules.

Les modalités peuvent être variées, tant en cyber qu'en action physique. Dans le domaine économique et scientifique par exemple, nous nous sommes rendu compte que certaines opérations d'espionnage en mode cyber pouvaient avoir pour intérêt d'accéder au cœur du réseau d'un certain nombre d'entreprises françaises. L'objectif peut être alors de capter des informations de nature industrielle, dans une logique de développement de capacités concurrentes et d'avantages stratégiques, mais aussi de se prépositionner dans le cadre de repérages en vue d'actions de sabotage.

Le défi, pour la DGSI, est de réussir à qualifier précisément les choses. Nous faisons toujours preuve de prudence quand il s'agit de déterminer à qui peut être attribué un événement. À la veille de l'ouverture des Jeux olympiques, par exemple, lorsque des attaques coordonnées ont été menées contre plusieurs points de desserte de notre réseau ferroviaire, nous nous sommes demandé à qui nous avions affaire. Menées le 26 juillet au matin, ces dégradations nuisaient aux vacanciers, aux spectateurs venant assister à la cérémonie d'ouverture, mais aussi à l'image de la France et de sa capacité d'organisation des Jeux. Elles pouvaient donc servir un acteur étatique ayant intérêt à s'en prendre à la France. Elles pouvaient aussi servir des acteurs hostiles à l'organisation d'un événement de cette nature – au regard de la mobilisation des ressources naturelles, de celle des services de l'État, de l'engagement sécuritaire –, par exemple

des mouvements que je qualifierai d'ultra-gauche car c'est en ces termes qu'on analyse en France la mouvance anarcho-autonome.

Notre défi est donc d'analyser les éléments auxquels nous avons accès – les éléments physiques que nous recueillons sur le terrain et la connaissance des modes opératoires d'attaque de nos adversaires – pour essayer au maximum de qualifier les choses. Sur le plan politique, ce n'est pas un sujet facile : il faut donc prendre le temps d'analyser les faits en les confrontant à ce que nous savons des modes opératoires de nos adversaires et en nous documentant sur leurs objectifs stratégiques. Nous y parvenons par le biais d'enquêtes en propre ou au travers d'échanges avec nos partenaires internationaux. Dans le cadre des investigations conduites *a posteriori*, après la commission des faits, nous nous appuyons sur ce qui apparaît au cours des enquêtes judiciaires et activons parfois les dispositifs de « renseignarisation » prévus par la loi : dans certaines circonstances, les autorités judiciaires sont autorisées à nous transmettre des éléments de leurs procédures, que nous intégrons ensuite dans nos enquêtes de renseignement.

Il s'agit d'un travail de précision qui nécessite que nous disposions de connaissances préalables – il faut comprendre les actions qui sont menées, connaître les modes opératoires et les objectifs de nos adversaires et être capables d'analyser les éléments soumis à notre constat dans ce contexte.

M. Loïc Kervran, président. Même lorsque l'attribution est certaine, la décision de la rendre publique est en soi un choix politique, car si l'on annonce avoir repéré l'action d'un État sans que cette déclaration soit suivie d'une réponse crédible, on s'affaiblit. Il existe d'autres canaux pour informer un État qu'on a identifié son action sans le dire publiquement.

Mme Céline Berthon. C'est d'ailleurs ce qui fait la grande différence entre l'action que nous menons en matière d'antiterrorisme et celle que nous menons en matière de contre-espionnage et de contre-ingérence. Dans le cas de l'antiterrorisme, les faits sont assez facilement attribuables. Pendant longtemps, nous avons été dominés par des logiques d'organisations transnationales qu'il était aisé de dénoncer. En revanche, lorsque les faits répondent à une logique de confrontation non armée entre États, il y a des choix d'attribution à effectuer qui relèvent, non pas tant de nos services, mais également de l'action diplomatique et politique.

M. le général de corps d'armée Aymeric Bonnemaison. Pour en revenir à la notion de continuum, tous les services de renseignement se sont transformés, passant d'une culture du « besoin d'en connaitre » – un travail en « fuseau » – à un besoin de partager et d'échanger, justement pour pouvoir mettre en relation les différents modes d'action qui s'exercent dans les différents espaces – cyber, physique et autres. Nous interagissons désormais beaucoup entre services : à la DRSD, nous sollicitons souvent Tracfin par exemple, ainsi que la direction nationale du renseignement et des enquêtes douanières, DNRED. Il y a eu une ouverture en interne, mais aussi entre services de renseignement.

Je peux illustrer la complexité de ce continuum avec l'exemple des nombreuses fuites de données sensibles que nous avons eues, en particulier dans l'industrie de défense. Dans ce type de cas, il ne faut surtout pas se précipiter. En premier lieu, contrairement à une idée répandue, toutes ces fuites ne sont pas d'origine cyber. Elles peuvent provenir d'un « *insider* », c'est-à-dire d'une personne de l'entreprise, de la structure ou de l'état-major, qui est soit

retournée, soit amenée pour des raisons personnelles à récolter des données pendant un temps assez long avant de les regrouper pour les mettre sur le *dark web*, essayer de les vendre ou tenter de nuire en les diffusant. Elles peuvent aussi provenir d'un vol d'ordinateur, dans une voiture ou devant une salle de sport – les petites compromissions font les grandes opérations. Et, en regroupant les informations, on peut aussi constater qu'il y a eu plusieurs vols, pas nécessairement dans l'entreprise ciblée mais chez ses sous-traitants, qui font apparaître une intention derrière des incidents en apparence isolés.

Il convient ensuite de prendre en compte l'aspect de la finalité. Les fuites de données peuvent se produire par exemple en pleine compétition sur un contrat export – elles visent alors à décrédibiliser la société concernée – ou au moment d'une levée de fonds pour une jeune entreprise. Elles peuvent aussi servir à faire diversion au moment où des actions sont tentées sur un champ plus physique.

Tout cela demande du temps. On ne doit pas se précipiter pour caractériser une menace émergente. Le phénomène des survols de drones par exemple, inclut un vaste éventail de situation, en partant du « tout-venant » anodin aux évènements les plus sérieux, dont certains peuvent appeler des suites judiciaires. Après quoi nous travaillons à l'imputation : nous essayons de remonter techniquement le fil, sachant que chacun essaie d'employer les moyens des autres pour nous leurrer. C'est ensuite que vient la phase de l'attribution, qui relève de choix politiques : on peut contacter directement le pays par le biais de l'ambassadeur pour lui signaler qu'on l'a vu ; on peut aussi rendre l'affaire publique, soit dans le cadre d'une organisation internationale comme l'Otan ou l'Union européenne, soit seul, dans différents cadres.

J'insiste vraiment sur la difficulté du sujet. Dans les médias, les choses vont toujours très vite. Notre travail n'est pas de courir derrière. Pardonnez-nous d'essayer de le faire posément, avec professionnalisme.

Quant aux actions de freinage dont vous parliez, elles ne sont pas simples à caractériser non plus. Certaines personnes peuvent en mener pour des raisons tout à fait légitimes et personnelles, comme la défense d'une cause – j'ai connu, sur certaines emprises militaires, des grenouilles très spécifiques qu'il ne fallait pas déplacer. Mais une action en apparence légitime peut aussi être téléguidée, ou récupérée par opportunisme par des pays étrangers.

M. Aurélien Saintoul (LFI-NFP). Monsieur le directeur, vous nous avez donné quelques chiffres. S'agissant des faits de sabotage, notamment des incendies dont on a beaucoup parlé ces derniers temps, disposez-vous de chiffres caractérisant une augmentation ?

Vous avez aussi évoqué la difficulté à imputer les attaques réputationnelles : est-on en revanche capable de mesurer leurs effets ? Je pense par exemple à Naval Group ou à Dassault.

J'ai ensuite une question sur Palantir qui vaut pour les deux services. Pourquoi la DGSI a-t-elle décidé de continuer à se fournir auprès de cette société alors que M. Nuñez avait jugé qu'il fallait y mettre un terme il y a déjà quelques années, et que l'Allemagne a choisi pour sa part ChapsVision ? La DRSD est-elle amenée à auditer les systèmes de Palantir auxquels recourt l'Otan – le système Maven, en l'occurrence – ou s'agit-il d'une prérogative exclusive du Comcyber ?

Enfin, s'agissant des ingérences électorales, *Le Canard enchaîné* s'est fait l'écho d'une réticence éventuelle de la DGSI à enquêter sur les ingérences qui ont ciblé les candidats Insoumis à Roubaix, Toulouse et Marseille. Je voulais vous donner l'occasion, madame la directrice générale, de démentir je l'espère cette réticence.

Mme Céline Berthon. Vous noterez, monsieur le député, que l'effet recherché par des manœuvres informationnelles alimente vos deux dernières questions. Notre rôle est justement de résister à ces manipulations.

S'agissant des incendies, je ne dispose pas ici de chiffres mais je peux vous indiquer des tendances. Puisque la lutte contre le terrorisme et les extrémismes violents entre dans notre champ de compétence, nous nous intéressons à toutes les radicalités qui peuvent conduire à des actions violentes – sabotage, incendies, voire actes qualifiés de terroristes. Notre pays a été confronté ces dernières années à plusieurs actions et projets d'actions motivés par des idéologies radicales qui ont pu passer par ce biais, comme l'attaque de pylônes électriques. Nous avons observé une logique de pics d'action, qui répondent souvent à des mots d'ordre. Nous constatons également une montée en puissance de l'antimilitarisme dans l'idéologie des groupes radicaux que nous surveillons. Les conflits actuels, tant russo-ukrainien qu'au Proche et Moyen-Orient, suscitent une mobilisation pour dénoncer la militarisation du monde et les discours en ce sens. Dans ce contexte, les incendies sont plutôt en augmentation, visant soit des cibles dans la BITD ou à proximité, soit des grands projets de construction – principalement des structures carcérales ou des centres de rétention administrative.

La manipulation informationnelle est extrêmement complexe à qualifier, en particulier au niveau de ses effets. Le SGDSN et Viginum, le service de vigilance et de protection contre les ingérences numériques étrangères, peuvent sans doute apporter des éléments à ce sujet.

Je précise qu'elle ne relève pas nécessairement d'une ingérence étrangère : la puissance des réseaux sociaux, la capacité de publication des plateformes, le recul dramatique des capacités de modération de plusieurs d'entre elles et la viralité de certaines publications alimentent le phénomène. D'où la difficulté à caractériser la chose et à mesurer ses effets.

Cela nous conduit toutefois à être particulièrement attentifs aux étapes clés de notre vie démocratique. S'agissant de votre question relative à l'article du *Canard enchaîné*, le champ d'action de la DGSI la fait contribuer à la prévention, à la détection et à la caractérisation des manœuvres étrangères étatiques. Nous sommes donc mobilisés dans le cadre du dispositif déployé par l'État pour la protection de nos échéances électorales, qui peuvent effectivement être ciblées – le sujet est largement documenté depuis la campagne de 2017. Il y a une différence sémantique qui n'est pas neutre entre ce qui relève de la lutte contre l'ingérence numérique étrangère – que couvre et définit très bien Viginum : c'est extérieur, mais pas forcément étatique – et ce qui relève de la lutte contre l'ingérence étatique dont s'occupe la DGSI.

S'agissant de Palantir, la DGSI a dû acquérir une brique logicielle en 2016, lorsqu'elle a été confrontée à l'enjeu d'un traitement massif de données, dans un contexte de forte exigence que je n'ai pas besoin de rappeler. Comme à l'accoutumée, le directeur général en place a étudié les alternatives disponibles et c'est un outil de Palantir qui répondait aux besoins identifiés. La DGSI a contractualisé pour l'utilisation de cet outil, dans des conditions strictement définies et dans une logique de contrôle des données traitées. C'était dès l'origine

une solution considérée comme temporaire, l'objectif étant de chercher une alternative souveraine, française ou européenne, qui puisse répondre aux besoins. C'est effectivement Laurent Nuñez, alors directeur général de la sécurité intérieure, qui a initié en 2019 la recherche d'un tel outil, qui n'existait alors ni en France ni en Europe. Alors que ce produit était encore en cours de développement, la DGSI a dû renouveler son contrat avec Palantir, pour éviter toute rupture dans sa capacité de traitement des informations et de réponse à l'exigence de ses missions. Le contrat a donc été renouvelé, oui, mais pour une durée limitée, dans l'attente que le nouvel outil soit effectivement prêt à l'usage.

M. le général de corps d'armée Aymeric Bonnemaison. S'agissant des incendies, je n'ai pas non plus de chiffres mais on observe effectivement une tendance antimilitariste, qui se traduit par du tractage et des manifestations, mais aussi par des actions un peu plus notables, revendiquées – comme dans le cas du transformateur électrique. Cette dynamique antimilitariste est clairement portée par la situation internationale. On l'a vue glisser d'une approche très propalestinienne et anti-Israël à une approche antimilitariste beaucoup plus générique, avec en toile de fond la question du service national. Cette tendance gagne en visibilité, sans forcément correspondre à un mouvement de fond dans la population : on constate en effet de notre côté un certain attrait pour les sujets de sécurité, au niveau du recrutement dans nos services ou dans les industries de défense.

S'agissant des attaques réputationnelles, la mesure de leurs effets est extrêmement difficile. On a tendance à utiliser des mesures de performance, comme le nombre de *likes* ou de partages, qui peuvent être le signe d'une écume très temporaire. En revanche, d'autres actions réputationnelles peuvent faire du mal sans être pour autant phénoménales – je mentionnais tout à l'heure le cas des fuites de données qui ciblent comme par hasard, en pleine démarche export, le pays concerné et les services chargés de faire des choix.

Enfin, la DRSD n'inspecte pas les réseaux militaires de l'Otan. C'est une chaîne organisée en interne qui s'occupe de ces choix-là.

M. Aurélien Rousseau (SOC). Vous avez évoqué le resserrement stratégique entre nos compétiteurs. Constatez-vous une convergence entre les différentes menaces – terrorisme, narcotrafic, vol de données, actions étatiques ? Des États jouent-ils la carte de l'hybridation par des canaux inhabituels, notamment par le narcotrafic ?

Par ailleurs, la situation politique aux États-Unis influe-t-elle sur vos échanges avec leurs services, qui sont essentiels pour notre capacité de détection des risques et de protection du pays ? Notre niveau de coopération avec notre plus grand partenaire est-il moins bon depuis quelque temps ?

Mme Céline Berthon. L'hypothèse de l'instrumentalisation des modes opératoires est une question importante.

Pour y répondre, nous pouvons nous fonder sur le diagnostic – précis, mécanique, chirurgical – des profils, des modes opératoires et des capacités de financement des auteurs que nous identifions, que l'attentat soit réalisé ou en projet. En 2026, nous avons malheureusement déjà connu un attentat et trois projets dans le domaine du terrorisme d'inspiration djihadiste. Leurs auteurs n'avaient que peu ou pas de capacités de financement, ce qui s'est d'ailleurs traduit par des modes opératoires très sommaires – l'usage du couteau. Nous observons que les auteurs ne parviennent pas à trouver des armes, recherchent des tutoriels d'explosifs et n'ont

pas forcément le savoir-faire pour les réaliser. Lorsqu'ils identifient un vendeur d'armes, soit ils n'ont pas d'argent – à la différence du narcotrafic et de la criminalité organisée –, soit ils essuient un refus. Dans le cadre d'un projet terroriste en effet, les fournisseurs d'armes peuvent être poursuivis pour des faits de complicité et s'exposer au même niveau de condamnation que les auteurs principaux. C'est là un effet redoutablement efficace des dispositions antiterroristes en France.

Nous n'observons donc pas de lien structurel entre le terrorisme, le narcotrafic et la criminalité organisée en France, même si nous restons vigilants. Certains phénomènes convergent, comme le rajeunissement et la digitalisation, mais on constate une stricte séparation entre les objectifs, les modes opératoires, les financements et les idéologies.

C'est moins vrai au niveau des États. Nous avons pu caractériser – et non imputer ou attribuer – le fait que certains États sont capables d'avoir recours à des moyens terroristes. C'est le cas, soyons clairs, de l'Iran. Premièrement, au cours de son histoire, l'Iran a peu mobilisé son appareil de renseignement pour venir frapper ses cibles stratégiques – lointaines et difficilement accessibles. Cela l'a conduit à mobiliser des intermédiaires, ce qui a pu mener à la réalisation d'actes violents à caractère terroriste. Deuxièmement, le recours à ces modes est un moyen de limiter le risque d'attribution et de pouvoir plaider le déni plausible quand une cible américaine, israélienne ou juive est touchée : cela permet d'éviter d'en porter la responsabilité directe et de se mettre à distance.

Le lien entre le terrorisme et l'action étatique est donc documenté, contrairement à ce qui se passe dans les domaines du narcotrafic et de la criminalité organisée. Il peut passer par des moyens cyber.

S'agissant du niveau de coopération des services, dans la situation actuelle, nos alliances stratégiques étaient effectivement susceptibles d'être questionnées. Chaque service est soumis aux priorités politiques de son administration, et les choix américains pouvaient conduire à dérouter des moyens. La priorité mise sur le narcotrafic était ainsi susceptible de peser sur notre coopération en matière de lutte antiterroriste, mais nous ne l'avons pas constaté. Il y a aussi dans ce genre de situations une possibilité de changement de correspondant et de perte d'habitudes de travail qui n'est pas neutre, mais nous ne l'avons pas davantage constaté pour le moment.

M. le général de corps d'armée Aymeric Bonnemaison. Pour nommer ces menaces, nous utilisons le filtre Tessco : terrorisme, espionnage, sabotage, subversion, crime organisé. S'agissant du terrorisme, nous sommes peu contributeurs : nous surveillons surtout ce qui se passe chez nous – la radicalisation éventuelle de nos personnels, voire les actions contre nos forces, par exemple au sein de l'opération Sentinelle. Pour le reste, nous percevons clairement une inflation des menaces d'espionnage, de sabotage et de subversion : tout cela est d'ailleurs mêlé. Nous sommes également très vigilants à l'égard du crime organisé, dont le spectre s'étend par le biais du numérique : il est facile aujourd'hui de recruter quelqu'un pour conduire une action, à l'aide d'internet et des cryptomonnaies.

Certaines personnes, également, ne sont pas conscientes d'être instrumentalisées par un État. Elles conduisent une action par conviction personnelle sans savoir qu'elles sont en fait orientées vers une cible ou agitées par un relais extérieur, qui peut œuvrer pour un État.

S’agissant des relations entre services, il existe historiquement un très bon niveau de coopération sur la sécurité des forces, un peu comme en matière de contre-terrorisme. Cela concerne nos forces déployées en opérations extérieures, ainsi que les menaces extérieures qui pourraient nous cibler sur le territoire national en raison de notre appartenance au monde militaire ou à la défense. C’est d’autant plus intéressant alors qu’émergent les menaces hybrides russes, qu’il s’agisse de faire face à une action imminente d’espionnage ou de sabotage, ou alors de caractériser les modes d’action et leur évolution – vous voyez ce que je peux gagner ainsi chez ceux qui sont proches de nos adversaires russes.

Je n’échange pas beaucoup en revanche, ce qui ne vous surprendra pas, dans le domaine de la contre-ingérence économique en matière de défense. Le général de Gaulle disait qu’un pays n’a pas d’amis, seulement des intérêts : c’est particulièrement sensible dans ce champ-là, et je ne vous cache pas qu’on n’avance pas beaucoup sur ce point dans nos échanges entre services.

M. Jean-Louis Thiériot (DR). Durant la guerre froide, les mouvements pacifistes anti-nucléaires avaient été très largement infiltrés par le KGB, voire par le Conseil œcuménique des Églises. Actuellement, dans la mouvance écologiste radicale – ultra-gauche pacifiste contestataire, ou ultra-droite de la *deep ecology* –, constatez-vous des ingérences de services étrangers qui ne nous veulent pas du bien ? Avez-vous le sentiment que cela augmente ? Est-ce cartographiable et mesurable ?

S’agissant de la prédation économique et des investissements étrangers en France, pouvez-vous préciser les modalités de votre coopération avec le service de l’information stratégique et de la sécurité économiques (Sisse) au sein du Comité de liaison en matière de sécurité économique, par exemple pour la détermination des participations ? Quelle est votre stratégie pour détecter les faux-nez dans ces prises de participation capitalistiques – ceux qui s’avancent pour cacher d’autres acteurs ? Quelle évolution constatez-vous dans la pratique de la *lawfare* ? Devrions-nous, en tant que parlementaires, être conscients de certaines évolutions législatives de nos compétiteurs, survenues récemment ?

Mme Céline Berthon. S’agissant des logiques associatives ou de mobilisation en défense d’une cause, nous ne constatons pas les liens que vous évoquez. Lorsqu’il y a une logique transnationale, entre des groupes ou associations présents en Europe, elle est plutôt de solidarité, de partage d’intérêts, de renfort lors de mobilisations. Elle est le fait d’initiatives individuelles ou associatives sans lien caractérisé avec des États à ce stade.

S’agissant des investissements étrangers, la DGSI et la DRSD agissent toutes les deux dans le cadre d’un ballet d’acteurs animés par la direction générale des entreprises et le Sisse en vue de la protection de notre patrimoine scientifique et technologique. Dans ce contexte, nous balayons tous les leviers qui peuvent être utilisés pour fragiliser nos entreprises. L’investissement et les logiques capitalistiques font partie des tout premiers risques et types de menaces. Nous devons donc être capables de détecter les moments de vulnérabilité capitalistique de nos entreprises, d’identifier les acteurs susceptibles de prendre des participations et d’actionner les dispositifs de blocage prévus par la loi pour empêcher une prise de participation préjudiciable.

Nous ne sommes pas des régulateurs de la compétition légitime économique. Nous empêchons la réalisation d'actions hostiles qui feraient perdre de manière déloyale des capacités à nos entreprises. Nous aidons à caractériser les investisseurs et à identifier les faux-nez – qui peuvent cacher des acteurs étatiques ou paraétatiques – pour permettre aux autorités de convocation d'activer le cas échéant des dispositifs de blocage.

S'agissant de la *lawfare*, notre vocation est d'identifier les vulnérabilités des entreprises que nous devons aider à protéger. Il peut s'agir de fragilités physiques : nous contribuons à des audits bâtimentaires, et nous détectons, prévenons, caractérisons, poursuivons si besoin et entravons toute mesure relevant d'une logique de prédation ou de démarchage physique. Mais pour ce qui est de la *lawfare* et de l'extraterritorialité au sens large, il faut être conscient que la granularité de la dissémination de ce mode d'action peut relever de schémas toujours plus avancés. Il est essentiel de nous documenter de manière régulière sur ces sujets.

Les instances de normalisation me préoccupent beaucoup, car elles peuvent être investies de manière très significative par des États disposant d'une force de frappe importante. En mobilisant des experts et des ressources et en prenant d'assaut toutes les instances de cette nature, ils peuvent contribuer à promouvoir et à imposer des normes bénéficiant à d'autres structures ou sociétés que les nôtres. Il s'agit à mon sens d'un enjeu majeur de vigilance et d'investissement, à l'échelle nationale, européenne et internationale.

M. le général de corps d'armée Aymeric Bonnemaison. S'agissant des mouvances actuelles, nous n'avons rien caractérisé, mais plus le phénomène s'amplifiera, plus il sera récupérable. L'attribution en revanche ne sera pas aisée car, contrairement à un soldat qui sait quelle cause il défend, l'action pourra être menée de façon inconsciente. Ces réseaux peuvent être approchés par des services extérieurs qui les inciteront à cartographier nos points sensibles pour savoir où frapper, et orienteront ou agiteront l'intentionnalité et la virulence à l'aide de fausses informations. Ce n'est donc pas un mode direct d'appropriation, mais plutôt un mode indirect d'influence. On ne doute pas que cela arrivera, à défaut d'être déjà engagé.

S'agissant de la prédation économique, nous sommes très sensibles, dans l'industrie de défense, aux sujets du quantique et de l'IA. En France, nous rencontrons une difficulté générale de passage à l'échelle, notamment pour trouver des fonds français et européens. Il est compliqué de refuser à un jeune l'extension de son activité sous prétexte qu'il devrait recourir à des fonds étrangers, alors qu'on n'a pas de fonds français à lui proposer. La question des fonds souverains dans lesquels investir est donc centrale si l'on veut se donner des capacités de développement et accompagner nos entreprises au moment du changement d'échelle.

La jeune génération est parfois plus clairvoyante que certains de leurs pairs plus anciens. Ces derniers peuvent être plus attachés aux intérêts du groupe international pour lequel ils travaillent qu'à la cause de leur nation, là où leurs homologues étrangers pensent d'abord à leur pays. Nous constatons que les jeunes entrepreneurs sont davantage sensibles aux enjeux de souveraineté, tant à un niveau national qu'européen, ce dernier échelon représentant à leurs yeux à l'échelle nécessaire à un marché viable dans certains domaines.

L'arsenalisation du droit (*lawfare*) est un phénomène en expansion : après les lois d'extraterritorialité américaines, c'est maintenant le tour des chinoises – notamment en ce qui concerne les terres rares. Elles entraînent des contrôles à l'export et à l'embargo, souvent relayés par des cabinets d'expertise et d'audit, pour la majeure partie anglo-saxons – il serait

bon, d'ailleurs, d'accompagner le développement de cabinets nationaux. Nous prévenons les entreprises, et nous les accompagnons lorsqu'un contrôle est déclenché sur la base d'une loi extraterritoriale. En effet, les investigations menées par les cabinets, notamment anglo-saxons, ne respectent pas toujours la loi. Ils fouillent beaucoup plus loin que nécessaire et, par souci de se libérer de cette charge, les entreprises ont tendance à donner beaucoup d'informations – au point de toucher à des secrets défense pour ce qui me concerne, mais également à des secrets concernant leurs brevets ou leurs stratégies commerciales. J'ai quelques cas en tête qui montrent combien ces cabinets sont intrusifs.

Il serait également important d'être très vigilant, et très présent au moment de la construction des normes et standards dans les organismes internationaux. Nous devons nous poser ces questions très en amont car, une fois qu'une norme qui nous dessert a été fixée, tout devient très compliqué.

Mme Céline Berthon. Nous vous parlons du monde de l'entreprise, mais il est essentiel de protéger aussi nos universités et nos laboratoires. Cela a fait l'objet de travaux dans le cadre de l'actualisation de la loi de programmation militaire (LPM).

L'université représente le début du savoir, et les laboratoires créent la continuité vers le savoir-faire de nos entreprises. C'est un domaine très investi par des pays qui ont des moyens d'action importants, comme la Chine. Il est très important d'identifier le risque, de l'accepter et de faire évoluer la culture de sécurité dans le cadre de la recherche.

Mme Catherine Hervieu (EcoS). Les signaux faibles, pris dans leur ensemble, permettent de mesurer l'ampleur de l'influence qui s'insinue dans notre société par le biais des médias, des réseaux sociaux et des personnalités publiques – je songe ici à la présence de Xenia Fedorova dans plusieurs milieux influents, alors même qu'elle est identifiée depuis des années comme étant une influence active au service de la Russie.

Les atteintes et les attaques sont avérées. Parmi leurs objectifs, l'atteinte à l'image de la France et à sa capacité de protection de la population et de ses intérêts. Je pense notamment à l'attaque contre la Poste pendant Noël, aux vols de données de santé dans les hôpitaux et récemment auprès d'Alan, mutuelle pourtant préconisée par l'État et vouée à être généralisée dans la fonction publique, ou encore aux attaques contre le ministère de l'intérieur ou les opérateurs téléphoniques. Plus globalement, c'est la confiance des citoyens envers la capacité de nos institutions à les protéger qui est atteinte. Cela affecte certains partis politiques, mais cela mène plus largement à la déstabilisation du pays.

Monsieur le directeur, vous avez évoqué la DefTech. Nous autres politiques et députés ne sommes pas forcément les plus exemplaires quant aux précautions à prendre : nous utilisons des applications de messagerie étrangères, nous avons beaucoup de rendez-vous aux abords de l'Assemblée, nous n'avons pas vraiment de formation, malgré la sensibilisation que nous vaut le fait d'être à la commission de la défense. Les élites de notre pays souhaitent agir pour la résilience nationale, mais n'appliquent pas elles-mêmes les mesures de précaution requises.

Quelles sont les principales vulnérabilités identifiées au sein des secteurs stratégiques et des infrastructures d'importance vitale ?

Comment s'organise la coopération entre les différents services de renseignement et de sécurité au niveau européen ?

Mme Céline Berthon. La DGSI est toujours à votre disposition pour mener des campagnes de sensibilisation, même si nous le faisons déjà régulièrement. Nous sommes en contact avec les services de l'Assemblée et nous avons des équipes dédiées, qui adaptent leur approche en fonction du public cible et prodiguent des conseils vraiment pragmatiques.

S'agissant de notre stratégie de couverture des domaines économiques et technologiques, nous n'avons pas la capacité de suivre toutes les entités françaises. Nous couvrons donc celles qui présentent les enjeux les plus forts, c'est-à-dire qui détiennent des savoir-faire ou des savoirs stratégiques qui, s'ils ne devaient plus exister en France, entraîneraient des vulnérabilités dans les chaînes de production stratégiques.

Nous sommes aussi engagés dans la protection, l'accompagnement et l'aide au développement d'un certain nombre de domaines stratégiques pour la vie ou l'avenir de la nation. Outre le numérique, l'IA et le quantique, il s'agit de champs fondamentaux comme l'électricité, l'alimentation, les médicaments ou encore le monde sanitaire. Dans ces secteurs, nous cartographions les sociétés qu'il importe de protéger et nous ciblons tous les types d'attaque dont elles peuvent faire l'objet : capitalistiques, cyber, humaines.

Ces dernières concernent, par exemple, un salarié qui laisse son ordinateur contenant des secrets de fabrication dans sa voiture. Elles peuvent aussi prendre la forme de logiques de débauchage par des entreprises concurrentes, qui récupèrent alors le savoir-faire du salarié. Il s'agit là d'une vraie stratégie menée de manière systémique par certains compétiteurs, qui y mettent des moyens financiers. Les déplacements à l'étranger sont un autre contexte de vulnérabilité : lorsque vous partez avec votre ordinateur et votre téléphone portable dans lesquels se trouvent toutes les données de la société, les passages de frontière et les chambres d'hôtel où le matériel est déposé sont des moments à forte intensité de risque.

Nous essayons donc de couvrir tous les champs opératoires possibles. Nous effectuons de la sensibilisation par des conférences, des déplacements, des rencontres régulières, des signalements sur les modes opératoires observés, mais aussi la diffusion d'une culture de sécurité. Nous publions notamment chaque mois sur les quelques réseaux sociaux où nous sommes présents un « flash ingérence » illustré par des conseils pratiques et des cas d'espèce.

M. le général de corps d'armée Aymeric Bonnemaison. Le champ des menaces est si vaste et évolue à une telle vitesse qu'on ne peut pas s'occuper de tout : il est donc impératif que tous les citoyens soient conscients de ces risques. Nous devons développer le niveau de vigilance en France, sans affoler mais en sensibilisant, et les compromissions doivent être déclarées – elles sont pour la plupart dues à des négligences.

La société change : une guerre cognitive s'opère, en particulier depuis les réseaux. Il faut donc développer l'esprit de vigilance et l'esprit critique. C'est l'un des dangers de l'IA : à force de la laisser se substituer à nos cerveaux, nous ne pourrons bientôt plus conserver le regard critique que nous portons sur ses réponses dans notre domaine d'expertise ou d'expérience. Petit à petit, nous allons nous laisser guider. C'est un vrai risque, car la base de données utilisée n'est pas forcément fiable et que l'algorithme ne vous explique pas comment il est arrivé à une décision.

Dans le domaine cyber, l'enjeu est le même que pour les militaires sur le champ de bataille : c'est la rapidité avec laquelle on intègre les innovations, qui est essentielle pour survivre. L'arrivée de Mythos, même si l'on ne connaît pas encore ses capacités réelles, montre bien qu'un jour les vulnérabilités de nos systèmes seront immédiatement détectables par des IA, alors qu'il fallait auparavant du temps pour trouver la faiblesse, déterminer comment l'utiliser, se prépositionner et rester sur le réseau. Aujourd'hui, nous nous trouvons dans une compétition permanente entre le bouclier et le glaive. Le danger surgit dans l'intervalle, quand le glaive a un coup d'avance, qu'il vient chercher vos vulnérabilités et piller vos données et qu'il faut être rapidement en mesure de le contrer.

C'est la raison pour laquelle nous devons avoir nos champions nationaux, capables de réinjecter très rapidement des solutions et d'adapter nos modes d'action – quitte à condamner temporairement un service à travailler en mode dégradé, le temps de monter en gamme et d'atteindre un niveau de protection supérieur. C'est un vrai défi et nous avons un travail d'explication considérable à mener sur ce sujet.

Mme Josy Poueyto (Dem). Les techniques d'algorithme, qui ont beaucoup évolué ces dernières années, seront encore amenées à connaître de grands bouleversements. Les techniques de cryptographie sont déjà particulièrement sophistiquées, et voilà que l'on parle désormais de chiffrement quantique. Si l'ordinateur quantique en capacité de menacer les chiffrements actuels ou de procéder à ses propres chiffrements n'est pas encore au point, la recherche s'intéresse déjà aux techniques post-quantiques afin de ne pas être en retard le jour où le quantique s'imposera. Il s'agit d'une anticipation nécessaire, même si les meilleurs spécialistes ne peuvent dire à quelle échéance cette révolution verra le jour. En tout état de cause, ce sont les données des services de l'État qui sont en jeu, tout comme la faculté de l'État à décrypter ce que d'autres acteurs veulent cacher.

Dans ce contexte ultra-compétitif, on s'emploie à récolter maintenant pour décrypter plus tard : les données peuvent conserver de la valeur en attendant le moment où il sera possible de les craquer. Ce phénomène n'est pas nouveau, mais il est en passe d'atteindre des niveaux inégalés jusqu'à présent.

Dans cette course folle, pouvez-vous nous dire où en sont vos services avec le quantique et le post-quantique ? À quelles conséquences vous attendez-vous ? Comment anticipez-vous dès aujourd'hui la nécessité de préserver durablement la confidentialité des données et les garanties fondamentales en matière de protection de la vie privée ?

M. le général de corps d'armée Aymeric Bonnemaison. L'arrivée du quantique n'est pas une surprise les armées qui l'ont anticipée, par exemple en soulignant le besoin d'un chiffrement post-quantique. Nous avons aussi en tête la possibilité que des pays concurrents aient capté et stocké des données pour tenter de les casser, et nous travaillons à l'étape d'après.

Il y a trois domaines qui intéressent la défense dans le quantique : le calcul, les communications – le quantique pourra les rendre intraçables et très difficiles à intercepter : il est donc important de savoir ce que nos adversaires potentiels développent – et enfin les capteurs – le quantique pourra permettre de détecter des éléments indétectables à l'heure actuelle, ce qui compliquera l'effet de surprise dans certaines actions militaires.

Avant même le risque que vous abordez, on peut aussi se demander ce que chacun d'entre nous donne déjà aux Gafam, aux géants du numérique. J'ai parfois le sentiment qu'on étudie beaucoup les services de renseignement nationaux, qui sont pourtant très contrôlés – notamment par vous – et qui ont une éthique certaine et une déontologie. Ce que vous donnez aux grands groupes quand vous téléchargez une application gratuite n'est guère protégé et souvent plus intrusif Ayant été Comcyber, je suis très sensible à la sécurisation des réseaux mais je sais aussi qu'il faut bien définir l'équilibre entre libertés publiques et sécurité, qui est compliqué à trouver. Au niveau des services de renseignement français, nous ne mobilisons pas de la technologie de masse comme on le voit dans les films : les choses sont beaucoup plus ciblées et contrôlées.

Mme Céline Berthon. Pour ma part, j'appréhende le quantique dans une logique de défense de ceux de nos champions nationaux qui sont bien positionnés sur ces sujets-là. Au titre du dispositif de protection du potentiel scientifique et technique de la nation, nous sommes très engagés dans la protection des travaux de recherche développés par des laboratoires et des universités françaises. Nous sommes plutôt bien placés dans ce domaine, et il est donc important que nous ne soyons pas pillés.

Nous anticipons aussi les effets sur nos méthodologies de travail. En tant que service de renseignement, nous avons besoin d'accéder à un certain nombre d'éléments et l'hypothèse de communications intraçables fait partie de nos préoccupations, puisque notre travail est justement de détecter les menaces, de les caractériser et d'entraver leur réalisation.

Aymeric Bonnemaison s'interrogeait sur l'équilibre observé entre ce qui est donné aux Gafam et ce qui est autorisé aux services de renseignement. J'ai la certitude que nous avons une déontologie, une éthique et un contrôle – exercé par les parlementaires et par des autorités administratives indépendantes – qui n'existent pas de la même manière du côté des Gafam.

M. Bernard Chaix (UDR). En parallèle des efforts industriels, la guerre moderne se gagne aussi grâce à la supériorité technologique. Dans ce contexte, les grandes puissances ont largement recours à l'espionnage industriel. Aux côtés de Bruxelles et Washington, Paris est devenu une cible privilégiée – on compterait plus de 10 000 agents étrangers en activité dans la capitale. Comme vous l'indiquez dans votre panorama de 2025 sur les ingérences touchant notre BITD, monsieur le directeur, nos adversaires portent un intérêt singulier à nos technologies de rupture telles que l'IA et le quantique.

Parmi les enjeux majeurs, il y a d'abord notre cyberespace. En 2024, l'Anssi révélait que 42 % des opérations de cyberdéfense visaient à riposter contre des attaques de groupes liés à la Chine, qui tentent de capter nos savoir-faire en ciblant prioritairement nos entreprises de haute technologie.

Cependant, la première des menaces d'ingérence demeure d'origine humaine – de l'ordre de 28 % du total en 2025. Nos compétiteurs tentent de débaucher nos ingénieurs et nos chercheurs. Cette guerre économique se mène en silence, discrètement, au travers d'approches via LinkedIn et de la part de cabinets de recrutement étrangers. Si nos fleurons savent bien se protéger, 80 % des menaces ciblent nos PME et entreprises de taille intermédiaire (ETI), plus vulnérables. C'est d'autant plus grave que de nombreux composants critiques de nos technologies de pointe proviennent de notre tissu de PME.

Quelles mesures de contre-ingérence sont prises pour protéger nos PME, alors que l'enjeu est immense et qu'elles sont fatalement plus vulnérables que nos fleurons ?

Pourriez-vous dresser un état des lieux du débauchage de nos experts et nous dire quels principaux compétiteurs le pratiquent et quelles méthodes ils emploient ? Ces dernières ayant beaucoup évolué, comment vos services s'y adaptent-ils ?

Mme Céline Berthon. Vous avez raison de mettre l'accent sur la vulnérabilité humaine, qui est un vecteur utilisé par nos compétiteurs, et sur la stratégie de débauchage qui vise à la fois nos enseignants-chercheurs et les salariés d'un certain nombre de nos entreprises.

Vous avez également raison de rappeler que la menace peut concerner à la fois de grands groupes, des PME et des ETI. Notre dispositif de contre-ingérence économique nous conduit à nous intéresser aux sociétés sur la base de leur savoir-faire stratégique, quelle que soit leur taille. Nous couvrons aussi bien de grands groupes du CAC40 que de toutes petites entreprises ainsi qu'un certain nombre de start-up, ce qui nous conduit à accompagner des sociétés durant tout le schéma de vie de leur activité.

Les logiques de débauchage utilisent parfois les mêmes ressorts que l'espionnage, où, pour avoir accès à une information qui nous intéresse, on mobilise chez la personne qu'on veut traiter des ressorts qui peuvent être idéologiques, financiers, de l'ordre de la rancœur ou encore de la compromission.

Quand donc on veut débaucher une personne qui détient un savoir-faire stratégique et qu'on a les moyens de l'acheter, on peut utiliser la motivation financière. Cela concerne des acteurs économiques qui ont une puissance de feu et d'investissement qui leur permet de surpayer, le cas échéant, les savoirs dont ils ont besoin. On peut utiliser aussi le vecteur de la rancœur ou de la rancune : on s'en prend à un salarié qui n'est pas satisfait de son sort dans son entreprise et qui est capable, pour se venger de son chef, d'aller bosser pour la concurrence. On peut aussi cibler des personnes qui ne sont pas détentrices d'un savoir-faire mais qui serviront de vecteur d'accès : une personne assez neutre dans la chaîne de production, mais qui conserve des relations avec ses anciens collègues et pourra vanter les conditions d'accueil de sa nouvelle société et attirer ainsi d'autres salariés.

Dans ce contexte, nous cherchons à développer la culture de sécurité, pour faire reculer la naïveté. Nous alertons les personnes qui se font démarcher sur des réseaux professionnels ou qui sont invitées à des salons ou dans des ambassades sur le fait qu'elles sont en réalité ciblées pour des raisons précises, et nous leur révélons la réalité cachée derrière les manifestations d'intérêt de leurs interlocuteurs.

Nous essayons aussi d'activer, lorsque c'est possible, en lien avec les employeurs, les clauses de non-concurrence prévues par le droit du travail ou des entreprises, ou encore des dispositions de déontologie. Enfin, lorsque des savoir-faire d'importance stratégique sont en jeu, ou des logiques de compromission, nous n'hésitons pas à recourir à de l'entrave administrative, voire judiciaire. C'est arrivé récemment dans le domaine de la recherche, y compris avec des qualifications assez lourdes lorsque nous avons réussi à caractériser la nature exacte des faits.

Dans ce contexte, nous mobilisons donc toute la gamme des réponses possibles. Nous sommes aussi amenés à faire des flash ingérence spécifiques sur les démarchages sur les réseaux sociaux, notamment dans le cadre des réseaux professionnels.

M. le général de corps d'armée Aymeric Bonnemaison. D'abord, monsieur Chaix, merci de vous référer à nos chiffres : je suis très heureux de voir que notre lettre d'information économique a été lue !

Les PME-ETI sont vraiment notre cœur de cible. La DRSD, intervenant dans le champ de la défense, a affaire à des populations et à des entreprises un peu plus sensibilisées que ce qui vient d'être évoqué, en particulier lorsqu'elles ont des systèmes classifiés qui ont nécessité des enquêtes administratives ou des avis d'habilitation. Cela étant, nous avons connu cette problématique, notamment dans le cas de pilotes qui allaient faire de l'instruction en Chine – un exemple qui a alimenté l'article 42 de la dernière LPM et qui a vocation à servir d'épouvantail en la matière. Il faut cependant intervenir finement : il ne s'agit pas d'interdire systématiquement à qui que ce soit d'aller travailler ailleurs sous prétexte qu'il a fait partie de telle entreprise. Nous regardons les spécialités en jeu au cas par cas. Récemment, nous avons ainsi dû entraver le départ d'un employé d'industrie doté d'une spécialité très fine qui partait à l'étranger.

M. Loïc Kervran, président. Nous en venons aux questions individuelles des députés.

M. Thomas Gassilloud (EPR). Déjà trois attentats déjoués ! Merci à tous deux de ce que vous faites face aux actions de nos adversaires.

Il ne faut pas oublier que nous pouvons aussi être en compétition avec nos alliés. Quelle est notre posture de défense face à eux ?

Nous avons voté récemment un état d'alerte de sécurité nationale : comment imaginez-vous la posture de la DRSD et de la DGSI en cas de crise majeure ? Madame la directrice, vous avez dit que les chefs de file devaient rester les mêmes en temps de crise : quelles sont vos craintes ? Il me semble que la DGSI contribue largement à la défense nationale et je ne vois pas d'échange possible.

Mme Sophie Errante (NI). Nous venons de voter l'actualisation de la LPM, et on entend parler d'une actualisation de la Lopmi (loi d'orientation et de programmation du ministère de l'intérieur). Je pense qu'elle est nécessaire : quel est votre avis à ce sujet ? J'espère en tout cas que la commission de la défense sera bien saisie, au moins pour avis.

M. Loïc Kervran, président. Je me permets d'insister sur la question de Thomas Gassilloud : pour qui connaît un peu le monde des services de renseignement, vos mots sur le respect des chefs de file, madame la directrice, ne peuvent que nous interpeller.

Mme Céline Berthon. Face à nos alliés, nous devons adopter une posture de responsabilité et peser à chaque fois ce que sont nos alliances et, si ce n'est nos méfiances, du moins nos points d'attention. À chaque échange avec nos partenaires, nous pesons nos intérêts respectifs et nous nous retrouvons sur des alliances de circonstance. Il peut ne pas y en avoir, ce qui ne signifie pas pour autant que nous sommes dans une logique d'adversité ; simplement, il faut se poser la question à chaque fois. Ainsi, si nous travaillons assez peu avec certains pays

en matière d'ingérence économique, nous sommes en revanche complètement alignés sur d'autres sujets.

S'agissant des chefs de file, je ne voulais pas faire peur. Je pense simplement qu'en temps de crise, il ne faut pas réinventer les choses qui fonctionnent. Notre domaine d'action étant assez discret, nous sommes méconnus, et pas assez diserts. Nous gagnerions probablement à développer notre pédagogie. Il faut en tout cas résister, le cas échéant, aux entreprises trop imaginatives : nous avons une communauté du renseignement particulièrement solide et mature, qui constitue une base saine en temps de crise.

S'agissant enfin de la Lopmi, la préparation à la conflictualité a conduit à une actualisation ambitieuse de la loi de programmation militaire. Le ministère de l'intérieur et la DGSI sont de leur côté confrontés à des enjeux de consolidation de leur savoir-faire et à des enjeux capacitaires. Si une loi doit permettre une actualisation des enjeux stratégiques du ministère de l'intérieur et des moyens qui vont avec – humains, technologiques, financiers, législatifs – je pense qu'il ne faut pas se l'interdire. C'est un projet qui ne m'appartient pas, mais nous aurons certainement matière à l'alimenter.

M. le général de corps d'armée Aymeric Bonnemaison. Concernant nos alliés, nous sommes loin d'être naïfs en matière de contre-ingérence dans le domaine de l'économie de défense. Les marchés sont de plus en plus gros, car beaucoup de pays réinvestissent dans la défense : cela entraîne des repositionnements d'États, y compris amis. Nous devons donc rester très vigilants sur ce sujet.

S'agissant des postures en temps de crise, l'exercice Orion 2026 a été particulièrement enrichissant. Lors de l'exercice Orion 2023, le ministère des armées était un peu regardé de loin. Cette année, le travail interministériel, sous l'égide du SGDSN, a été extrêmement constructif : nous assistons à une véritable prise de conscience, et des modes de fonctionnement sont en place qui permettent d'établir des connexions et de conscientiser certains ministères encore très éloignés des sujets de sécurité.

La posture intermédiaire, présente dans l'actualisation de la LPM, va être également intéressante. Elle permet de travailler sur des modes gradués, car il n'est pas réaliste d'agir dans une logique de « tout ou rien ». Nous sommes passés à une menace un peu plus permanente, avec des moments de pics : pouvoir doser son effort de riposte reste important.

Quant aux chefs de file, ne déstabilisons pas ce qui marche. En tant que chef d'un service de renseignement – et je l'ai déjà vécu dans mon poste précédent –, quand on regarde les menaces qui pèsent sur notre champ de responsabilités, on se désole un peu ; mais quand je me compare à d'autres pays, je me console. Il y a des choses qu'on ne met pas en avant en France, mais le renseignement a gagné en maturité dans tous les domaines – le contrôle des services, les échanges, la coordination, la fluidité. Soyons clairs, cela n'a pas toujours été comme ça. La prise de conscience actuelle en matière de sécurité est également intéressante : nous devons l'étendre à nos concitoyens, sans faire peur.

Je rebondis d'ailleurs sur le dernier point : s'il y a une actualisation de la Lopmi, ce sera intéressant de voir si je suis invité ! *(Sourires.)*

M. Loïc Kervran, président. Merci d'avoir montré que, face au glaive qui mêle tant de modes d'actions civils et militaires, le bouclier aussi sait être hybride. Nous retiendrons, mon général, votre belle formule pour désigner ces acteurs qui cherchent à nous soumettre sans nous combattre.

La séance est levée à onze heures cinq.

*

* *

Membres présents ou excusés

Présents. - Mme Delphine Batho, M. Hubert Brigand, M. Bernard Chaix, M. Yannick Chenevard, Mme Sophie Errante, M. Yannick Favennec-Bécot, M. Guillaume Garot, M. Thomas Gassilloud, M. Frank Giletti, M. José Gonzalez, M. David Habib, Mme Catherine Hervieu, M. Laurent Jacobelli, M. Pascal Jenft, M. Loïc Kervran, Mme Laure Lavalette, M. Didier Lemaire, Mme Patricia Lemoine, M. Julien Limongi, Mme Alexandra Martin (Alpes-Maritimes), M. Thibaut Monnier, M. Karl Olive, Mme Josy Poueyto, Mme Natalia Pouzyreff, Mme Catherine Rimbert, M. Aurélien Rousseau, M. Aurélien Saintoul, M. Sébastien Saint-Pasteur, M. Jean-Louis Thiériot, Mme Sabine Thillaye, M. Romain Tonussi, M. Antoine Valentin

Excusés. - Mme Valérie Bazin-Malgras, M. Christophe Bex, M. Matthieu Bloch, M. Frédéric Boccaletti, M. Manuel Bompard, Mme Caroline Colombier, M. Michel Criaud, Mme Geneviève Darrieussecq, M. Moerani Frébault, M. Damien Girard, M. Daniel Grenon, M. Jean-Michel Jacques, M. Bastien Lachaud, Mme Nadine Lechon, Mme Lise Magnier, Mme Michèle Martinez, Mme Anna Pic, Mme Mereana Reid Arbelot, Mme Marie-Pierre Rixain, M. Arnaud Saint-Martin, Mme Isabelle Santiago, M. Mikaele Seo, M. Bertrand Sorre, M. Boris Vallaud, M. Laurent Wauquiez

Assistait également à la réunion. - Mme Corinne Vignon