ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Mercredi
18 mars 2026
Séance de 9 heures 30

Compte rendu n° 7

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures trente.

M. le président Philippe Latombe. Nous accueillons ce matin le général Dominique Luzeaux, que nous sommes très heureux de recevoir à Paris alors que le commandant de l'Otan dont il relève est basé à Norfolk, en Virginie.

Notre commission d'enquête cherche à mesurer la vulnérabilité des administrations publiques vis-à-vis de technologies et d'infrastructures digitales développées ou opérées par des acteurs extra-européens, ainsi que la vulnérabilité des données conservées par ces administrations. Comment évaluez-vous l'état de la dépendance numérique française dans le domaine de la défense ? Au sein de l'Otan, comment concilier coopération entre États et souveraineté dans le domaine numérique ?

Avant de vous laisser la parole, je vous remercie de nous déclarer tout intérêt public ou privé de nature à influencer vos déclarations et je rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

(M. Dominique Luzeaux prête serment.)

M. Dominique Luzeaux, général de division, chargé de mission « transformation numérique » auprès du commandant suprême allié pour la transformation de l'Otan. C'est un honneur et un plaisir d'être reçu par la représentation nationale pour discuter de ce sujet très important.

La France a toujours joué un rôle clé dans le numérique : c'est le pays qui a inventé le Minitel ; le pays de Louis Pouzin, inventeur du protocole pour les réseaux à commutation de paquets, qui a fortement inspiré celui utilisé par internet ; c'est aussi celui de la carte à puce et du premier micro-ordinateur. Nous possédons de très nombreuses compétences, à tel point qu'on peut s'étonner de notre dépendance aux serveurs de Google, Microsoft et Amazon. La question est donc de savoir comment mettre ces compétences au service de la réduction des dépendances structurelles et des vulnérabilités systémiques dans le secteur du numérique.

Le point critique réside dans notre capacité à choisir nos dépendances et à y répondre plutôt qu'à les subir. On parle beaucoup de souveraineté ; je préfère parler de choix de dépendances et d'indépendance. Si l'on analyse ces aspects à l'aune de différents critères – démographiques, énergétiques, technologiques, militaires, économiques –, aucun pays n'est réellement souverain sur l'intégralité d'une chaîne de valeur. L'important est donc d'être capables de maîtriser nos dépendances critiques. Pour cette raison, je parlerai plutôt de résilience souveraine hiérarchisée : l'objectif n'est pas la souveraineté totale, mais la réversibilité.

Le numérique n'est pas un secteur parmi d'autres : c'est une condition d'existence de la puissance publique, de la continuité de l'État et de la liberté d'action nationale. Il en va de même en matière de conduite des opérations militaires : le numérique n'est plus un simple soutien à la manœuvre, mais la condition d'existence de la conduite des opérations. Ainsi, la rupture d'un maillon du flux numérique – depuis les capteurs jusqu'aux effecteurs – ne dégrade pas seulement la manœuvre, elle l'annule. C'est là un des grands changements de ces dernières décennies.

Il nous faut donc identifier nos dépendances et en évaluer le niveau – critique, sensible, négociable – pour y apporter des réponses proportionnées. Cette hiérarchisation nécessite un arbitrage et un calendrier, ainsi que des engagements politiques dans la durée. On ne saurait remédier aux vulnérabilités systémiques dans le domaine numérique en quelques mois ou années, par une action coup de poing : seul un engagement politique durable permettra d'apporter une réponse crédible à l'échelle du pays ou du continent.

Je ne m'attarderai pas sur la dimension économique et administrative de la vulnérabilité française en matière numérique, à laquelle d'autres auditions sont consacrées. Je me concentrerai plutôt sur les aspects opérationnels et militaires, car la défense et la sécurité sont des domaines dans lesquels les dépendances numériques peuvent induire des vulnérabilités systémiques auxquelles nous devons être en mesure de réagir.

À titre d'exemple, la pénurie de semi-conducteurs a des conséquences sur le maintien en condition opérationnelle de certains systèmes ainsi que sur leurs coûts. Faut-il, par conséquent, constituer des réserves stratégiques de composants numériques ? Cette question est particulièrement centrale s'agissant d'équipements militaires dont la durée de vie est de plusieurs décennies, alors que le rythme de développement et d'évolution des technologies, notamment électroniques et informatiques, se compte plutôt en années.

Les infrastructures numériques critiques – les data centers, notamment – sont également des cibles vulnérables. On l'a constaté très récemment aux Émirats arabes unis et au Bahreïn, mais ce fut également le cas en Ukraine, où certains ont été bombardés ou neutralisés par les Russes dès les premiers jours du conflit. Plusieurs câbles sous-marins ont aussi été sectionnés en mer Baltique.

Au-delà de cette dimension *hardware*, c'est-à-dire matérielle, qui renvoie à l'empreinte physique importante du numérique, la vulnérabilité concerne aussi les *softwares*, les logiciels. J'en veux pour preuve le détournement du BGP (*Border Gateway Protocol*, ou protocole de passerelle frontière), qui a permis aux Russes de perturber le routage du trafic européen à plusieurs reprises.

L'intelligence artificielle (IA) est un autre sujet clé. Le fait qu'elle soit très largement utilisée pour les actions de ciblage dans le cadre du conflit en cours en Iran soulève des interrogations concernant les données d'entraînement, les biais éventuels ou encore les seuils d'engagement pour lesquels on accepte de confier un rôle important à l'IA. Se pose aussi, par conséquent, la question du cadre législatif et juridique à définir pour traiter ces aspects.

J'ai évoqué la vulnérabilité des data centers face aux attaques cinétiques, mais il faut aussi avoir conscience qu'un data center sans documentation et sans compétences de supervision ou d'opération est une coquille vide. Cela m'amène à la question de la formation et de la structure étatique à développer pour pouvoir opérer, maintenir, isoler, dégrader, voire reconstruire, en cas de rupture, les infrastructures ou les capacités numériques. Le domaine cyber est couvert par le Comcyber (commandement de la cyberdéfense) et l'Anssi (Agence nationale de la sécurité des systèmes d'information), mais peut-être faudrait-il créer, dans le domaine numérique, des organisations qui permettront de disposer des compétences nécessaires en cas d'urgence – je songe par exemple à la réserve opérationnelle. La réponse à une dépendance numérique n'est pas que technologique : elle passe aussi largement par la formation et par le maintien des compétences.

La commande publique est clairement un instrument de puissance pour tenter de réagir aux dépendances numériques. Peut-être faudrait-il aussi définir un cadre permettant de déroger à certaines règles ordinaires de mise en concurrence, à l'instar de la procédure qui permet, lorsque des intérêts essentiels de la sécurité de l'État sont en jeu, de renoncer à la mise en concurrence systématique tout en respectant le cadre légal. L'objectif n'est nullement de contourner le droit, mais de prévoir une forme d'exception numérique en tant que de besoin. Cette possibilité devrait faire l'objet d'une doctrine d'emploi explicite : elle ne serait pas utilisée systématiquement, mais uniquement en cas de nécessité. Une exception stratégique pourrait ainsi s'appliquer en cas de danger numérique majeur pour la continuité de l'État.

Je l'ai dit, la souveraineté numérique s'inscrit dans une logique de temps long : il faut assurer la continuité de l'effort politique, assumer les choix collectivement, sanctuariser quelques briques critiques et entretenir notre base industrielle. Je fais ici référence au périmètre national, mais il nous faut aussi construire cette souveraineté au niveau européen si nous voulons être compétitifs et crédibles à l'échelle mondiale. Or, pour reprendre l'adage, on ne prête qu'aux riches : il sera plus simple de faire entendre notre voix en Europe si nous possédons des compétences reconnues.

Sans prétendre mettre le numérique sur le même plan que la politique de dissuasion nucléaire, force est de constater que cette dernière n'est pas fondamentalement remise en cause à chaque changement de majorité. De la même façon, peut-être faut-il concevoir le numérique comme un projet structurant qui, sans forcément être apolitique, devrait faire l'objet d'une certaine continuité dans sa conduite.

Pour en venir aux technologies, le numérique s'organise en quatre grands paquets. Le premier, sur lequel on se focalise à tort, englobe les données. Le second concerne la connectivité, c'est-à-dire les infrastructures de transport de ces données – câbles, câbles sous-marins, fibres, réseaux de téléphonie mobile 5G et 6G, etc. Le troisième regroupe le stockage et la manipulation des données, c'est-à-dire les systèmes d'exploitation, donc le cloud – aussi bien le *core cloud*, le cloud public, que le *edge cloud*, le nuage à la périphérie. Le quatrième a trait à l'exploitation des données, grâce aux applications et à l'intelligence artificielle.

Si l'un de ces paquets est vulnérable, l'ensemble de la chaîne le devient. C'est ce que l'on appelle, en cybersécurité, le *Swiss cheese model*, le modèle du fromage suisse : comme dans un gruyère, il y a des trous, mais l'important est de veiller à ce que ces derniers ne soient pas alignés afin d'éviter les vulnérabilités systémiques. Pour prendre une autre image, si le numérique était une maison, les données correspondraient à l'eau, la connectivité aux canalisations extérieures, les systèmes d'exploitation et le cloud à l'évier et à la plomberie, et les applications et l'IA aux robinets : pour que la maison soit habitable, il faut que tout fonctionne. Par ailleurs, chacun de ces paquets, en plus de son empreinte physique et logicielle, est associé à des enjeux de formation et de réglementation qu'il convient également de prendre en compte.

S'agissant des infrastructures matérielles, une première source de vulnérabilité potentielle concerne les matières premières, leur disponibilité ou leur recyclage. Les réseaux de communication en sont une autre – câbles sous-marins et terrestres, radio, téléphonie, satellites. S'y ajoutent les data centers et les infrastructures de calcul, indispensables pour développer les champs du HPC (*High Performance Computing*, calcul de haute performance) et de l'intelligence artificielle. Enfin, n'oublions pas que le numérique est très gourmand en énergie, d'autant que les GPU (*Graphics Processing Units*, processeurs graphiques) utilisés pour l'intelligence artificielle consomment bien davantage que les CPU (*Central Processing Units*,

ou processeurs) auparavant utilisés dans les ordinateurs. Une grande quantité d'énergie est donc nécessaire, non seulement pour faire fonctionner les infrastructures, mais aussi pour extraire la chaleur qu'elles émettent.

Un autre point de vulnérabilité concerne les composants critiques, comme les semi-conducteurs ou les routeurs, aussi appelés éléments de réseau – actifs ou passifs. Par exemple, les routeurs intelligents, dont le nombre est en constante augmentation, permettent certes de créer des réseaux un peu partout et de les configurer à l'envi, offrant une flexibilité d'emploi accrue aussi bien dans le civil que dans le militaire, mais les nombreux logiciels qu'ils intègrent sont autant de sources de vulnérabilité, puisqu'ils peuvent être pilotés à distance. Or ils sont majoritairement d'origine chinoise ou américaine, ce qui en fait une dépendance clé dans les réseaux.

Pour ce qui est du logiciel, une surveillance particulière devrait s'exercer sur les systèmes critiques de type Scada (système de contrôle et d'acquisition de données), utilisés pour piloter les infrastructures industrielles. Ces systèmes sont en effet vulnérables aux attaques de *malwares* – logiciels malveillants. Chacun a en tête l'exemple du ver informatique Stuxnet, déployé il y a quelques années pour infecter des éléments physiques qui contrôlaient les centrales nucléaires iraniennes. Il y a beaucoup à faire pour pallier cette vulnérabilité systémique.

Concernant les modèles d'intelligence artificielle, l'*open source* est à la fois une réponse et une vulnérabilité. Lorsque des services de très bas niveau, téléchargés par de très nombreux développeurs, sont programmés par une toute petite communauté d'informaticiens russes employés par l'entreprise Yandex, la question de la vulnérabilité se pose de façon aiguë. Or tous les utilisateurs ne sont pas capables de vérifier l'intégralité des codes proposés, et le très grand nombre de communautés qui existent, notamment sur la plateforme GitHub, ne permet pas d'effectuer une revue exhaustive desdits codes.

La réglementation, la formation et la recherche sont également des éléments centraux. Que ce soit au sein du ministère des armées et des anciens combattants ou à l'Otan, nous nous efforçons d'améliorer le niveau de compétences des décideurs et des opérateurs dans les domaines de la cybersécurité et du numérique.

On pourrait en outre travailler à un programme national de migration des données publiques hébergées sur le cloud ainsi qu'à la consolidation et à la montée en puissance de clouds souverains, en s'appuyant sur des solutions certifiées SecNumCloud comme OVHcloud, Outscale ou Scaleway. Peut-être faut-il également être plus coercitif pour favoriser l'utilisation desdites solutions. Pour l'heure, un acheteur public qui souhaite opter pour un service de cloud ne peut pas, en théorie, privilégier une solution plutôt qu'une autre. Les dernières directives insistent certes sur l'importance de la souveraineté, mais elles n'en font qu'un critère de choix parmi d'autres et ne garantissent donc pas que c'est la solution satisfaisant ce critère qui sera retenue.

Pour ce qui est des composants critiques, le European Chips Act, le règlement européen sur les semi-conducteurs, permet de prendre certaines actions, mais il importerait aussi de renforcer la recherche et le développement sur le recyclage – et de construire des usines. La littérature scientifique fait état de procédés qui, en laboratoire, permettent de recycler certaines terres rares ; il s'agit désormais d'industrialiser ces processus et de soutenir les investissements en ce sens. Les routeurs, quant à eux, sont principalement détenus par les acteurs américains Cisco Systems et Juniper Networks, ou par l'entreprise chinoise Huawei. Ils

prendront une importance clé au moment du passage à la 6G, ce qui soulève d'ailleurs aussi la question des normes – j'y reviendrai.

Un autre enjeu majeur concerne la création d'un réseau d'État sécurisé et résilient. Nous sommes déjà dotés du RIE (réseau interministériel de l'État) ; il faudrait l'étendre aux fonctions publiques territoriale et hospitalière ainsi qu'aux OIV (opérateurs d'importance vitale) si nous voulons assurer la résilience globale et la continuité d'action de l'État.

Je faisais tout à l'heure la distinction entre *core cloud* et *edge cloud*. Le premier correspond aux data centers que chacun connaît. En la matière, la France s'efforce, par le biais d'offres comme Bleu ou S3NS, d'opérer un transfert de technologie depuis les *hyperscalers* – les géants mondiaux du stockage et de la gestion des données – vers des sociétés nationales. Le second désigne le fait de distribuer la capacité de calcul au plus près des capteurs. Dans ce domaine, les principaux *hyperscalers* ambitionnent d'être en mesure, d'ici quelques années, de proposer les services qu'ils fournissent actuellement pour le cloud public dans les montres connectées ou tous les produits concernés par l'IoT (*Internet of Things*, l'internet des objets). C'est une des solutions envisageables, mais ce n'est pas forcément la meilleure d'un point de vue technique : d'autres, qui reposent sur une approche *bottom up,* pourraient lui être préférées. Dans ce domaine, l'Europe pourrait prendre l'initiative et développer des solutions peu gourmandes en énergie. Il s'agit là d'un champ de recherche et d'un enjeu industriel d'une importance considérable : à l'horizon 2030, avec le développement de la 6G et de l'IoT, il faudra être présent sur le *edge cloud*.

Le même constat vaut pour les protocoles et les architectures de réseau. Le développement du *edge cloud*, typiquement, ne nécessite pas seulement des infrastructures physiques, mais aussi de nouveaux protocoles en *peer to peer*, très décentralisés et très distribués. Des travaux sont également en cours pour développer des réseaux très mobiles, comme les MANet (*Mobile* Ad hoc *Networks,* réseaux mobiles *ad hoc)* ou des réseaux entre voitures, autant d'usages auxquels les solutions actuellement proposées par les grands *hyperscalers* ne sont pas véritablement adaptées. Il y a donc là une occasion dont la France et l'Europe pourraient s'emparer. Les États-Unis l'ont d'ailleurs bien compris et commencent à se pencher sur ces sujets.

Au-delà de ces aspects technologiques, il est nécessaire de développer la formation initiale et continue et d'exploiter les talents existants, notamment à travers les réserves opérationnelles. La France doit également investir les organismes de régulation et de normalisation de la 6G, de l'intelligence artificielle ou encore de la blockchain. De manière générale, la réduction de nos dépendances numériques passera par une triple démarche : former, réguler et financer.

Je précise par ailleurs ne pas avoir d'information à propos de l'enveloppe budgétaire qui pourrait être allouée à tous les éléments que j'ai évoqués. Ce sera évidemment un point important : il ne sera pas forcément possible de tout faire. En tout état de cause, reconstruire une certaine indépendance numérique dans tous les domaines qui nous paraissent critiques prendra entre cinq et dix ans, ce qui pose à nouveau la question des alternances politiques éventuelles. Cela supposera aussi des partenariats entre public et privé, avec des amorçages publics. Créer et développer une filière industrielle est un travail de longue haleine. À mon sens, toutefois, la question n'est pas tant de savoir si la France peut se permettre d'investir dans la souveraineté numérique que de savoir si elle peut se permettre de ne pas le faire, au risque de découvrir la réponse au pire moment.

Le questionnaire que vous m'avez transmis comporte plusieurs questions précises.

Vous vous interrogez d'abord sur la façon dont les technologies numériques et l'IA ont transformé la stratégie militaire et les formes de conflictualité, et sur les principales applications d'IA en cours de développement dans le secteur de la défense. Sur ce dernier point, il faudrait poser la question à l'Amiad (Agence ministérielle pour l'intelligence artificielle de défense), qui a été créée après mon départ de la France il y a deux ans et demi. Du point de vue de l'Otan, en tout cas, l'intelligence artificielle est utilisée pour les systèmes d'armes, pour l'autonomie – en particulier des drones et des missiles intelligents –, ainsi qu'en matière de renseignement et d'analyse. Elle apporte une valeur ajoutée dans le traitement massif de données, dans la prédiction de menaces et dans le ciblage – on le constate, des deux côtés, dans le conflit qui oppose Israël et les États-Unis à l'Iran. Elle est aussi utilisée en cyberdéfense – détection d'intrusions, contre-mesures automatisées, détection de *deepfakes* (hypertrucages) – et sert d'aide à la décision, en particulier pour améliorer les *wargamings* (jeux de guerre) et tester des scénarios. Elle contribue également à la maintenance prédictive. Elle peut donc être utilisée dans chacun des quatre paquets que j'évoquais. De manière générale, elle assiste les décideurs et accélère les processus, tout en permettant d'éviter une saturation des opérateurs, qui sont confrontés à une quantité croissante de données.

Vous demandez également comment sont assurées la maîtrise des principales vulnérabilités et la résilience des activités critiques de l'État, et quels sont les acteurs et dispositifs clés de la stratégie nationale de cybersécurité. Parmi ces acteurs, il y a d'abord l'Anssi, chargée de la politique et de la réponse ; le SGDSN (secrétariat général de la défense et de la sécurité nationale), qui exerce la tutelle sur l'Anssi et assure la coordination ministérielle dans ce domaine, en matière civile et militaire ; ainsi que le Comcyber, rattaché à l'état-major des armées, qui gère la défense des systèmes d'information militaires et la conduite des opérations. Les missions de renseignement sont assurées par les directions générales de la sécurité intérieure (DGSI) et de la sécurité extérieure (DGSE), rattachées respectivement au ministère de l'intérieur et à celui des armées et des anciens combattants. Pour ce qui est des dispositifs, je mentionnerai la stratégie nationale de cybersécurité 2026-2030, qui prolonge la Revue nationale stratégique, le Livre blanc sur la défense et la sécurité nationale, la loi de programmation militaire, ou encore la directive NIS 2 (*Network and Information Security*, sécurité des réseaux et des systèmes d'information), qui renforce la posture cyber.

Vous souhaitez aussi connaître les grands projets en cours lorsque je présidais l'Agence du numérique de défense (AND), de sa création en 2021 à mon départ à l'automne 2023, ainsi que les défis organisationnels qu'ils posaient.

En matière d'infrastructures numériques, nous conduisions un projet de réseau de communication résilient et unifié pour la défense, ainsi que des projets de cloud de niveaux restreint et secret. L'Agence jouait aussi le rôle de maîtrise d'ouvrage de plusieurs systèmes d'information : de commandement et de contrôle – pour le renseignement militaire et la conduite des opérations –, d'administration et de gestion – pour la gestion des ressources humaines ou des hôtels et restaurants du ministère –, ou encore un système d'information logistique – pour assurer la logistique interarmées, les approvisionnements pétroliers, la maintenance navale et aéronautique, etc. Ces projets étaient conduits en adaptant des logiciels existants, ou, à défaut, en en développant de nouveaux, par le biais de la contractualisation et de la mise en concurrence, conformément au code de la commande publique.

Les défis étaient d'abord d'ordre technique et tenaient à la complexité des systèmes d'information et à la nécessité d'assurer la sécurité des données. La reprise de l'existant était

également un sujet d'attention et une source de coûts élevés : récupérer les anciennes données – ce qui est indispensable, notamment dans des domaines comme la maintenance ou les ressources humaines –, n'est pas toujours facile, surtout si elles sont stockées dans des formats qui ne sont plus compatibles avec les nouvelles technologies.

Une autre difficulté consistait à acquérir la compétence nécessaire pour assurer la maîtrise d'ouvrage de systèmes d'information complexes – la Cour des comptes signale d'ailleurs le même problème pour les systèmes d'information interministériels. Dans le même ordre d'idées, il fallait disposer d'effectifs et de compétences suffisants pour opérer en interne ou pour maîtriser l'apport de tierces maintenances applicatives. Des compétences spécifiques sont également nécessaires pour concevoir un cloud, mais également pour l'opérer – c'est le CloudOps – et pour définir les politiques financières adéquates – c'est l'approche FinOps. Pour maîtriser les coûts d'un cloud, en particulier quand il est opéré par une tierce partie, il faut en effet être capable d'en définir précisément la politique d'utilisation.

Vous m'interrogez ensuite sur le Commissariat au numérique de défense (CND), créé en septembre 2025. Il a pour objectif d'accroître la cohérence en rassemblant la gouvernance, qui relevait anciennement de la DGNum (direction générale du numérique et des systèmes d'information et de communication), la conception et le développement, qui relevaient de l'AND, et l'aspect opérationnel, géré par la Dirisi (direction interarmées des réseaux d'infrastructure et des systèmes d'information) – le *build* et le *run*, pour parler en termes informatiques. Sa création me semble de nature à renforcer la cohérence du pilotage de la transformation numérique du ministère des armées et des anciens combattants. Sans doute conviendrait-il désormais de créer une inspection du numérique, rattachée directement au ministre pour garantir son indépendance, afin qu'elle évalue les résultats du CND et propose des inflexions si nécessaire.

D'autres questions portaient sur le déploiement du cloud au sein du ministère des armées et des anciens combattants. En la matière, un des principaux enjeux est clairement celui de la sécurité. Dans le cadre de ma mission au sein de l'Otan, je travaille sur les mêmes types de clouds, de niveaux restreint et secret, que ceux qui nous occupaient à l'AND. Nous devons notamment veiller à la localisation, au cloisonnement et à la classification des données, ainsi qu'à la gestion et à l'identité des accès (IAM, *Identity Access Management*). Dans ce domaine, il existe des solutions technologiques, comme le *zero trust*, ou l'absence totale de confiance. Sans doute connaissez-vous la MFA (*Multi-Factor Authentification*, authentification multifacteur) ; le *zero trust* va plus loin, puisqu'il analyse non seulement le périphérique et le réseau utilisé, ou encore le mode d'accès à une application, mais aussi le comportement de l'utilisateur : si une même adresse IP formule des demandes d'accès depuis Paris, la Chine ou les États-Unis à quelques minutes d'intervalle, le système demandera une validation supplémentaire. C'est cette philosophie que nous essayons d'implanter, à l'Otan comme au ministère des armées et des anciens combattants, afin d'améliorer la protection.

Un autre sujet concerne la rémanence des données : il est important, pour le ministère, de pouvoir garantir l'effacement complet des données.

À cela s'ajoutent des enjeux opérationnels. Par exemple, un système d'information doit pouvoir continuer d'opérer en environnement dégradé. Les plus vieux d'entre nous ont connu l'époque où le téléphone se coupait dans les tunnels ; cela n'arrive quasiment plus jamais, mais les ruptures de connectivité sont très fréquentes dans la conduite des opérations. Il faut pouvoir continuer à travailler dans ces conditions, d'où l'importance de travailler à la fois avec

le *core cloud* et le *edge cloud*, pour gagner en agilité et pouvoir passer d'un système d'information à un autre en cas de rupture sur un réseau.

Le questionnaire évoque également le référentiel français SecNumCloud. Celui-ci a des limites : son coût de mise en œuvre est élevé, les solutions certifiées sont encore assez peu nombreuses, et, surtout, son niveau d'exigence n'a pas d'équivalent européen, ce qui pose problème pour l'exporter et répondre aux appels d'offres internationaux. Les exigences qu'il liste peuvent en outre avoir des interprétations diverses. Comme vous le rappelez, j'ai évoqué, dans un article paru dans la *Revue Défense Nationale*, la différence qui peut exister entre souveraineté et confiance. Il en va de même pour la notion de contrôle. Dans l'absolu, celle-ci implique le respect d'un cahier des charges spécifique. En cela, le SecNumCloud a l'avantage de proposer un cahier des charges explicite, qui permet de savoir précisément ce qu'une solution certifiée est capable de faire.

Vous m'interrogez sur le choix, par l'Otan, d'avoir recours à la plateforme d'intelligence artificielle Maven Smart System Nato (MSS Nato) de Palantir. L'Organisation comprend trois grandes structures : le quartier général et les deux commandements stratégiques – l'un pour la transformation, l'ACT (*Allied Command Transformation*), où je suis affecté, et l'autre pour les opérations, l'ACO (*Allied Command Operations*). En décembre 2024, l'ACO, estimant qu'il souffrait d'une rupture capacitaire, a émis une urgence opérationnelle en vue de se doter d'un outil qui lui permettrait d'améliorer la conduite des opérations. Conformément au mécanisme de consensus qui régit le fonctionnement de l'Otan, les trente-deux nations ont voté pour expérimenter le Maven Smart System de Palantir, avec qui a été conclu un contrat d'un an assorti de quatre tranches conditionnelles. Ce contrat, notifié le 25 mars 2025, s'appliquera donc potentiellement jusqu'en 2030. Parallèlement, un programme, intitulé SA for MDO (*Situational Awareness for Multi-Domain Operations,* connaissance de la situation pour opérations multidomaines), est en cours de définition au sein de l'Otan. Il permettra de spécifier les outils et processus dont l'Organisation devra se doter d'ici à 2030. Pour le dire brutalement, c'est donc le programme qui doit permettre de savoir quel outil remplacera Maven Smart System. Sauf si Palantir remporte la compétition qui sera lancée à cette occasion, MSS n'a donc pas vocation à être utilisé par l'Otan de manière définitive.

Quant aux données manipulées dans le cadre du contrat avec MSS, il s'agit de celles qui sont mises à la disposition de l'Otan par les nations. Elles sont de niveau secret et sont stockées dans des data centers isolés et cloisonnés.

Je ne suis pas en mesure de répondre à votre question relative à l'utilisation de logiciels de Palantir par la DGSI.

Le ministère des armées et des anciens combattants, quant à lui, a lancé le programme Artemis.IA, dont la réalisation industrielle a été confiée à la *joint-venture* ou coentreprise Athea (Atos-Thales) à l'époque où je dirigeais l'AND. Cette solution est désormais utilisée pour différents cas d'usage par la direction du renseignement militaire et par d'autres acteurs. Elle pourrait tout à fait répondre à certains besoins de l'Otan.

Enfin, vous me demandiez si des mécanismes similaires à ceux qui s'appliquent à l'exportation de matériels de guerre existent pour encadrer la dissémination des technologies numériques développées pour la défense française. La réponse est oui : ce domaine est soumis à la réglementation des biens à double usage, qui régit les applications civiles susceptibles d'être utilisées à des fins militaires. C'est le service des biens à double usage de la DGE (direction générale des entreprises) qui en est responsable.

M. le président Philippe Latombe. Les stratégies de cybersécurité américaine, canadienne et française présentées ces derniers jours portent sur des champs différents et se révèlent parfois orthogonales. Les États-Unis considèrent par exemple la cybersécurité comme un outil de puissance qu'on peut confier au secteur privé en permettant à ce dernier de mener des opérations offensives sur des réseaux communs. Comment l'Otan perçoit-elle ces divergences et compte-t-elle, dans ce contexte, atteindre le consensus que vous avez évoqué ?

Comment l'Otan entend-elle obtenir du renseignement cyber alors même que les États-Unis ont considérablement réduit le budget de la Cisa (*Cybersecurity and Infrastructure Security Agency*, l'Agence de cybersécurité et de sécurité des infrastructures), qui avait notamment fourni à la France, bien en amont des Jeux olympiques, des informations de très bonne qualité qui lui avaient permis d'anticiper les menaces ? Dans quelle mesure l'Otan et les pays européens dépendent-ils de la Cisa ?

M. Dominique Luzeaux. Les stratégies de cybersécurité sont effectivement très différentes d'un pays à l'autre, car elles sont guidées par la politique. Celle des États-Unis fait suite à la stratégie de défense nationale publiée l'année dernière : elle obéit à la logique Maga (*Make America Great Again*, « rendre sa grandeur à l'Amérique »), qui consiste à utiliser autant que possible les ressources industrielles américaines. Les Européens, et la France en particulier, ne partagent pas cette approche.

C'est tout l'enjeu des débats en cours à l'Otan – même si ces discussions portent en réalité sur les systèmes propres à l'Otan et répondent donc à une vision plus technique que politique, ce qui facilite les convergences. Pour rappel, le fonctionnement de l'Otan est le suivant : au moins 90 % des capacités sont apportées par les différentes nations ; pour le reste, l'Otan se charge, à travers les fonds communs, d'assurer le liant entre les différents systèmes quand cela est nécessaire. La même remarque vaut pour le renseignement : en cas d'opération, les nations apportent leurs renseignements et l'Otan opère une fusion des informations dans le cadre de la Cyber SA (*Cyber Situational Awareness*, ou connaissance de la situation cyber), ce qui permet à l'ACO de disposer d'une connaissance globale de la situation. Ce sont aussi les nations qui fournissent les moyens cyber défensifs – et *a fortiori* offensifs, l'Otan ne développant aucun moyen de cette nature.

Mme Cyrielle Chatelain, rapporteure. Vous avez indiqué qu'un programme est en cours pour remplacer le système développé par Palantir. Qui le dirige ? L'entreprise Palantir joue-t-elle un rôle de conseil dans ce cadre ?

Par ailleurs, les données stockées dans les data centers dans le cadre du contrat avec MSS sont-elles chiffrées, notamment lors de leur traitement ?

M. Dominique Luzeaux. Le programme SA for MDO est en cours de définition : des exigences opérationnelles ont été définies et validées par le Conseil de l'Atlantique Nord (ou *North Atlantic Council*, NAC), mais les spécifications sont toujours en cours de rédaction et n'ont pas encore été approuvées. Le programme n'étant pas encore lancé officiellement, aucun directeur n'a pour l'instant été nommé. Je peux en revanche affirmer que Palantir n'a aucun rôle de conseil dans le processus. L'entreprise répond uniquement à l'expérimentation menée par l'Otan dans les locaux de l'ACO.

Lorsque l'Otan développe un programme, le processus est rythmé par des franchissements de jalons. En l'occurrence, la première étape a consisté à demander aux équipes techniques, pilotées par l'ACO, de définir des exigences opérationnelles – en France, ce rôle

reviendrait à l'état-major des armées. Ces exigences ont ensuite été validées par les trente-deux nations – elles passent par divers comités, notamment militaires et financiers, avant de remonter jusqu'aux ambassadeurs qui siègent au NAC. Nous sommes actuellement dans la phase de rédaction des spécifications, assurée par des équipes techniques de l'ACT, de l'ACO et d'autres structures. Une fois ce travail achevé, il devra lui aussi être validé par les différents comités et approuvé par le NAC. Ce n'est qu'alors que le programme sera lancé pour réalisation.

À ce travail de développement en interne peuvent s'ajouter des RFI (*Requests For Information,* ou consultations pour information) – à distinguer des RFP (*Requests For Proposal*, c'est-à-dire des appels à proposition).

Les données manipulées dans le cadre du contrat avec MSS étant de niveau secret, elles sont effectivement chiffrées en conséquence. Le *hardware* de Palantir se trouve à l'intérieur du data center de l'ACO et a été récemment homologué. Il répond donc à diverses exigences relatives à la manière dont il est connecté – ou non – à certains réseaux et à la façon dont il est opéré. Les données contenues dans la mémoire interne de ce *hardware* ne sont pas nécessairement chiffrées, mais, contractuellement, toutes les données appartiennent à l'Otan et seront détruites si le matériel quitte le data center – d'où, comme je l'indiquais, l'importance, pour les ministères des armées, de pouvoir garantir un effacement complet des données.

Mme Cyrielle Chatelain, rapporteure. Vous avez précisé que le choix de Palantir avait été validé à l'unanimité. Est-ce parce qu'il n'y avait pas d'autre proposition ?

Pour revenir sur les données, j'imagine qu'au-delà du *hardware*, Palantir utilise aussi des logiciels de traitement et effectue de la maintenance ou des mises à jour. Ce sont plutôt ces opérations qui pourraient susciter l'inquiétude : n'y a-t-il pas nécessairement des points de contact entre Palantir et les données de l'Otan ?

M. Dominique Luzeaux. Le choix de Maven Smart System a nécessité plusieurs étapes : l'ACO a d'abord émis une urgence opérationnelle – signifiant ainsi le besoin de trouver une solution sous quelques mois, voire semaines –, puis le NAC a approuvé le choix d'une *single source* (approvisionnement unique), c'est-à-dire l'absence de mise en compétition. Le MSS a alors été sélectionné pour conduire l'expérimentation. Il n'est pas pour autant devenu une capacité pérenne de l'Otan : ce choix sera précisément l'objet du programme SA for MDO, qui est en cours de spécification.

Les mises à jour effectuées dans le cadre de cette expérimentation sont régulières, mais pas automatiques, et beaucoup moins fréquentes que dans d'autres versions de Maven utilisées par des industriels européens ou par d'autres organisations. Elles obéissent en outre à un principe de compartimentalisation et de segmentation : nous surveillons les points de contact potentiels entre les ingénieurs de Palantir et les personnels de l'Otan, et nous ne mélangeons jamais le *control plane* et le *data plane* (le plan de contrôle et le plan de données), si bien qu'un ingénieur qui effectue un contrôle de haut niveau n'a pas accès aux données – exactement comme pour SecNumCloud. Tous ces éléments sont inclus dans le dossier d'homologation Nato Secret. Enfin, contractuellement, donc juridiquement, toutes les données injectées ou créées appartiennent à l'Otan, et non à Palantir.

Mme Cyrielle Chatelain, rapporteure. À la lumière des prises de position de son fondateur, j'ai des doutes sur le respect du cadre légal par Palantir. Je continue par ailleurs de penser qu'il y a nécessairement des contacts entre son outil et les données traitées.

L'expérience montre qu'il n'est pas toujours possible de revenir en arrière à l'issue d'une expérimentation. Ainsi, la DGSI renouvelle régulièrement ses contrats avec Palantir, dont les logiciels sont également utilisés par plusieurs länder allemands. Nous sommes ici face à un opérateur dominant, dont le fondateur exprime des vues politiques hostiles au modèle européen et démocratique. Le fait qu'une telle entreprise occupe une place si stratégique dans le domaine des armées et de la sécurité intérieure constitue-t-il un risque pour la sécurité nationale ?

M. Dominique Luzeaux. Votre première remarque renvoie à la question de l'exfiltration des données. Tout l'objet de l'homologation, qui implique un ensemble d'analyses précises, est de s'assurer que cette exfiltration est impossible. On peut ne pas faire confiance au contrat, au cadre juridique ni à l'analyse technique, mais le fait est que des analyses sérieuses ont été effectuées.

La réversibilité des données est effectivement un concept auquel la plupart des Européens qui votent au sein de l'Otan tiennent énormément. Le MSS de Palantir est un outil qu'on peut programmer rapidement et utiliser pour connaître une situation en vue de la conduite d'opérations – pour produire des cartes, par exemple –, mais d'autres solutions, davantage dédiées au commandement et au contrôle ou susceptibles de répondre aux mêmes besoins que MSS, existent. La solution Artemis.IA en fait partie, tout comme SitaWare, solution européenne produite par Systematic, que les armées françaises utilisent momentanément dans le cadre du SIA C2 (Système d'information des armées – commandement et contrôle).

L'ancienneté de Palantir est à la fois un avantage et un inconvénient : en matière de système d'information, le fait de partir en premier est certes une bonne chose, mais, dans le même temps, les cycles technologiques sont très rapides. La plateforme MSS a déjà plus de dix ans : des solutions plus récentes pourraient être mieux à même d'intégrer, par exemple, les changements induits par l'intelligence artificielle. J'ai donc toute confiance dans la capacité de certaines solutions européennes à répondre aux futures consultations de l'Otan.

Mme Cyrielle Chatelain, rapporteure. Vous avez évoqué, dans certaines de vos publications, les difficultés que les situations d'oligopole peuvent générer à court et moyen termes. Encore une fois, le fait qu'un opérateur comme Palantir aspire à une position de monopole pose-t-il un problème de sécurité nationale ?

Vous expliquez par ailleurs que les décisions de l'Otan sont prises de manière consensuelle. Cela signifie-t-il qu'elle ne pourra pas avoir recours aux logiciels de Palantir si la France s'y oppose ?

M. Dominique Luzeaux. Tout à fait : une décision ne peut pas être approuvée si un pays s'y oppose. Des négociations peuvent alors prendre place – mais vous connaissez cela aussi bien que moi. Pour rappel, l'Otan est constituée d'une composante militaire, l'IMS (*International Military Staff,* staff militaire international) et d'une composante civile, le staff international (IS), où se tiennent des négociations politiques entre les différentes nations. On dit souvent que, l'Otan, ce sont les États-Unis, plus le Canada, plus les trente autres, c'est-à-dire l'Europe – même si cette dernière ne présente pas toujours un front uni. En tout cas, les décisions n'y sont pas prises de façon bilatérale et les États-Unis n'y occupent pas la même place qu'ailleurs. Le principe du consensus, qui fait quelquefois traîner les choses, permet d'introduire de l'inertie dans le processus, donc d'éviter que des décisions soient prises sur un coup de tête.

Pour en venir à votre première question, la place de Palantir au sein de l'Otan n'est pas un fort enjeu pour la sécurité nationale de la France, qui possède ses propres outils pour assurer sa sécurité. Il est vrai que, lorsqu'elle interviendra dans une opération sous le commandement de l'Otan, la France utilisera les produits de ce dernier, mais cela n'aura pas forcément d'implication directe sur sa capacité d'action. Le ministère des armées et des anciens combattants n'utilise pas Maven Smart System.

Mme Cyrielle Chatelain, rapporteure. Je songeais plutôt à la DGSI.

Dans l'un de vos articles paru dans la *Revue Défense Nationale*, vous écriviez que l'« offre oligopole du cloud questionne à court et moyen termes ». Dans un autre domaine, Palantir est un acteur doté d'une puissance importante – traitement massif de données, surveillance de masse, voire, d'après certaines enquêtes, fichage de citoyens américains –, dont le fondateur se considère comme un acteur politique, prend pour cible le modèle démocratique européen et, non content d'appartenir à un oligopole, a pour objectif de détenir le monopole sur le marché. En tant que spécialiste disposant d'une longue expérience, et pas seulement à l'Otan, pensez-vous que le fait de nouer un partenariat étroit avec ce type d'entreprises présente un risque en matière de sécurité et de dépendance ?

M. Dominique Luzeaux. Le ministère des armées et des anciens combattants n'est pas en partenariat avec Palantir. Je ne peux pas répondre pour le ministère de l'intérieur : il faudra interroger la DGSI sur ce point.

C'est précisément pour les raisons que vous avez évoquées que nous devons développer des solutions européennes ou nationales, afin de devenir de véritables acteurs dans ce domaine. Lors de mon passage au ministère des armées et des anciens combattants, j'avais ainsi notifié le contrat d'accélération de l'industrialisation d'Artemis.IA, suivi, un an plus tard, du contrat d'industrialisation. Ce programme continue d'être développé, utilisé et enrichi par le ministère, car nous souhaitons disposer non seulement d'une solution nationale, mais aussi d'un produit compétitif, susceptible d'être exporté et de remporter des compétitions internationales. D'autres solutions européennes auraient aussi leur place sur le marché, comme SitaWare de Systematic.

Si Artemis.IA n'existait pas, je serais bien plus gêné pour vous répondre. En l'occurrence, toutefois, nous possédons un produit qui satisfait nos armées, qui est régulièrement enrichi, et qui pourrait tout à fait répondre à des besoins de l'Otan.

M. le président Philippe Latombe. L'Otan est-elle perçue par les États-Unis comme un outil de puissance qu'ils peuvent utiliser pour imposer leurs solutions technologiques ? Chacun se souvient qu'ils ont demandé aux pays européens de prendre en charge une part plus importante des dépenses militaires de l'Organisation et qu'ils ont vendu leurs avions F-35, dont le système de vol induit une certaine dépendance, à plusieurs pays membres. Le principe de l'interopérabilité ne conduit-il pas de fait à s'aligner sur des technologies et des normes américaines, y compris en matière de réseaux – routeurs, câbles et probablement satellites ?

Quelles mesures sont prises, dans le cadre de la réallocation des moyens financiers, pour remédier à ce tropisme technologique américain ?

M. Dominique Luzeaux. Le fait de porter à 5 % du PIB les budgets consacrés à la défense devrait justement permettre à l'Europe de développer et d'imposer des solutions.

Vous avez insisté avec raison sur la notion de normes : la France et l'Europe doivent prendre une place beaucoup plus importante dans les instances de normalisation, qu'elles régissent les réseaux, les matériels, les logiciels ou tout autre élément clé en matière de dépendance numérique. Siéger dans ces instances permet d'influer sur les normes *de jure* ; cela coûte des effectifs sans bénéfice immédiat, mais c'est un investissement essentiel pour éviter de devenir dépendants à l'avenir. Parallèlement, développer des solutions compétitives est indispensable pour ne pas se trouver écrasé par des normes *de facto*, c'est-à-dire des normes qui s'imposent sur le plan industriel – ces discussions existaient déjà dans les années 1980.

Les États-Unis n'imposent pas leurs solutions par le biais de l'Otan. Simplement, pour remporter des compétitions, il faut être en mesure de proposer des solutions au marché, ce qui demande un investissement préalable. La hausse de leurs budgets de défense devrait aider les Européens à gagner en compétitivité – même si, j'en conviens, cela ne se fera pas en un jour.

Mme Cyrielle Chatelain, rapporteure. Un débat a cours aux États-Unis sur la place de l'IA dans les prises de décision. Il semble faire émerger la volonté de procéder à des frappes sans intervention humaine. Les États-Unis demandent-ils l'implantation d'un tel système au sein de l'Otan ?

M. Dominique Luzeaux. Non. L'Otan obéit au principe du HITL (*Human In The Loop*, l'humain dans la boucle) : aucune décision n'est automatisée de bout en bout.

Mme Cyrielle Chatelain, rapporteure. Le programme Artemis.IA est-il utilisé par d'autres pays européens ?

M. Dominique Luzeaux. Pas à ma connaissance, mais la *joint-venture* y travaille. Le ministère des armées et des anciens combattants a d'ailleurs organisé ce mois-ci une présentation, à laquelle a été conviée une délégation du quartier général de l'Otan, d'Artemis.IA et des capacités françaises. Cette démarche s'inscrit dans la volonté de montrer ce que la France est capable de faire dans ce domaine.

Mme Cyrielle Chatelain, rapporteure. L'utilisation de l'IA en matière de défense doit-elle être soumise à un cadre éthique, semblable à celui que s'est imposé Anthropic et qui l'a conduit à refuser de participer à des tirs de missiles sans intervention humaine ou à des opérations de surveillance de masse ?

M. Dominique Luzeaux. Je ne peux que répondre par l'affirmative. J'ai évoqué les problèmes juridiques posés par l'utilisation de l'IA dans les systèmes d'armes. Un cadre juridique et éthique est donc indispensable. L'analyse juridique (le *battle damage assessment*) qui sera menée à l'issue des conflits en cours aura d'ailleurs un rôle à jouer dans la définition de ce cadre.

Mme Cyrielle Chatelain, rapporteure. D'après plusieurs articles, l'aéronef F-35 ne peut fonctionner de façon autonome que pendant trente jours : au-delà, il faut se connecter au logiciel de maintenance pour effectuer des mises à jour. Confirmez-vous cette information ?

M. Dominique Luzeaux. Je ne sais pas répondre à cette question.

M. le président Philippe Latombe. Si vous pouviez modifier l'approche française du numérique pour atténuer nos dépendances à des technologies non européennes, quels seraient les deux domaines dans lesquels vous investiriez immédiatement ? De la même façon, quels

sont les sujets d'avenir sur lesquels nous devrions nous pencher dès maintenant pour éviter les dépendances de demain ? Je pense par exemple à l'informatique quantique.

M. Dominique Luzeaux. Effectivement, je n'ai pas abordé le quantique, mais ce secteur fait déjà l'objet d'investissements qu'il faut absolument poursuivre – dans les calculateurs, la cryptographie, ou encore les capteurs. Par exemple, même si l'on en parle encore peu, le développement de magnétomètres et de gravimètres quantiques devrait très rapidement permettre de contourner le problème du brouillage GPS. Le champ du PQC (*Post-Quantum Cryptography*, ou chiffrement post-quantique) mérite également d'être investi pleinement.

Pour ma part, j'investirais immédiatement dans les réseaux résilients, indispensables pour assurer la continuité des fonctions essentielles de l'État – je songe en particulier aux fonctions publiques hospitalière et territoriale – et dans le cloud à la périphérie, qui est amené à devenir un différenciant clé d'ici quelques années.

En matière de cybersécurité, il nous faut absolument investir pour mieux protéger les Scada et les objets connectés, qui sont notre point de vulnérabilité majeur. Il est ainsi tout à fait possible, par déplacement latéral, de pénétrer dans le système d'information d'une mairie après avoir pris le contrôle d'un feu de circulation. L'IoT offre des fonctionnalités formidables aux utilisateurs, mais il constitue un champ de vulnérabilité gigantesque.

M. Vincent Thiébaut (HOR). La France dispose d'un vrai savoir-faire en matière de réseaux, dont témoigne par exemple l'histoire du projet Rita (Réseau intégré des transmissions automatiques). Quel est le degré de dépendance d'un programme comme Scorpion (Synergie du contact renforcé par la polyvalence et l'infovalorisation) ?

Le cloud de combat fait partie des piliers du Scaf (système de combat aérien du futur). Son interopérabilité avec les systèmes de l'Otan, qui implique indirectement une ouverture à des normes américaines, présente-t-elle un risque ?

À la lumière du conflit ukrainien et de la volonté exprimée par le général Schill de territorialiser l'armée et de se rapprocher des industriels pour utiliser certaines technologies civiles comme les drones, comment envisagez-vous la question de l'interopérabilité entre des systèmes civils et des systèmes militaires qui, par nature, sont plutôt propriétaires et fermés ? Y voyez-vous un potentiel de vulnérabilité et un enjeu de souveraineté ?

Plusieurs sites alsaciens de la ligne Maginot anciennement utilisés par l'armée de l'air, notamment celui de Drachenbronn, ont été conçus de façon à bénéficier d'une redondance énergétique et de liaisons. Dans une logique de cloud souverain, certaines de ces bases pourraient-elles être réaffectées – il me semble par exemple qu'une réflexion est en cours à l'Otan pour constituer une base de retrait depuis Ramstein ?

M. Dominique Luzeaux. Le cloud est un élément clé : comme je l'indiquais, sans numérique, les manœuvres s'interrompent. Or, sans les plateformes, le numérique ne sert à rien, et vice-versa : nous avons besoin des deux, tout comme nous avons besoin à la fois de jambes et d'un système nerveux pour marcher. Il est donc indispensable de nous positionner sur le cloud de combat, qui fait partie des composantes du système global, si nous voulons être indépendants. Dans le même état d'esprit, nous devons participer à l'élaboration des normes de l'Otan : si certains renoncent à exercer une influence en la manière, d'autres peuvent imposer

leurs vues. En revanche, si chacun tente d'influer, des discussions s'engagent : c'est un bras de fer, ni plus ni moins.

S'agissant de l'interopérabilité entre le militaire et le civil, l'évolution de la technologie va en ce sens : les systèmes seront de moins en moins propriétaires et fermés et de plus en plus ouverts et modulaires. L'utilisation et la maintenance en condition opérationnelle des systèmes fermés et propriétaires est devenue beaucoup trop onéreuse pour qu'il en aille autrement. L'évolution des opérations obéit d'ailleurs à la tendance décrite par le général Schill, c'est-à-dire à l'approche M2MC (multimilieux multichamps) – MDO, dans le langage de l'Otan –, qui repose sur la convergence des effets militaires et la synchronisation avec les organisations civiles. On le constate clairement, la frontière entre le militaire et le civil est désormais brouillée.

Cette interopérabilité technique entre civil et militaire présente à la fois des avantages et des inconvénients. Pour maîtriser des systèmes ouverts et modulaires, il faut développer des compétences spécifiques, d'où l'importance de mettre l'accent sur la formation et la recherche, mais également sur la réglementation et la normalisation – ou standardisation. Or, si la France et l'Europe sont bien positionnées en matière de réglementation, elles ont des efforts à fournir en matière de normalisation : siéger dans les instances qui définissent les normes, que ce soit celles de l'Otan ou celles du secteur civil, sera capital à l'avenir.

Enfin, la question de la souveraineté énergétique est effectivement fondamentale.

Mme Cyrielle Chatelain, rapporteure. Vous décrivez l'Otan comme un espace d'influence. Chacun perçoit le changement très significatif à l'œuvre aux États-Unis, qui vont jusqu'à menacer des membres de l'Otan et à publier une stratégie de défense nationale affirmant très clairement la priorité donnée à l'Amérique et la volonté de dissuader les pays qu'ils considèrent appartenir à leur sphère d'influence de collaborer avec d'autres nations. Constatez-vous, depuis l'attaque du Venezuela et les menaces à l'égard du Groenland, une collaboration plus forte des Européens entre eux, ou au moins une volonté de prudence vis-à-vis des États-Unis de Donald Trump ?

M. Dominique Luzeaux. Clairement, le changement d'administration aux États-Unis a provoqué un électrochoc global, qui a incité l'Europe à se ressaisir et à développer ses propres solutions. Même si le processus ne fait que commencer et bien que l'Europe ne se positionne pas à proprement parler contre les États-Unis, l'augmentation de ses budgets de défense devrait l'amener à jouer un rôle plus important au sein de l'Otan. C'est d'ailleurs la volonté du président Trump : à l'entendre, l'Europe doit assumer sa propre défense. Au-delà des déclarations politiques, l'Otan est aussi le théâtre de discussions militaires, qui sont d'une nature assez différente. Néanmoins, depuis le 20 janvier 2025, on perçoit clairement la volonté de l'Europe de prendre davantage son destin en main.

M. le président Philippe Latombe. La place de la France au sein de l'Otan a-t-elle changé depuis l'arrivée au pouvoir de Donald Trump ? Son autonomie stratégique affirmée peut-elle lui permettre de gagner en influence, par exemple en promouvant ses propres systèmes, comme Artemis.IA, afin de regagner en indépendance ?

M. Dominique Luzeaux. La France est clairement reconnue pour son excellence militaire et technologique. Sa capacité de dissuasion nucléaire lui confère aussi une position particulière. À nous, désormais, de développer une base industrielle qui nous permettra d'influer aux niveaux national, européen et mondial.

M. le président Philippe Latombe. Merci beaucoup pour vos réponses. Si l'actualité vous inspire des remarques supplémentaires que vous souhaiteriez porter à notre connaissance, n'hésitez pas à nous les communiquer par écrit.

La séance s'achève à onze heures.

Membres présents ou excusés

Présents. – M. Éric Bothorel, Mme Cyrielle Chatelain, M. Philippe Latombe, M. Hervé Saulignac, M. Vincent Thiébaut