ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mercredi
26 mars 2025
Séance de 16 heures 30

Compte rendu n° 55

SESSION ORDINAIRE DE **2024-2025**

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

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures trente-deux.

M. le président Jean-Michel Jacques. Mes chers collègues, nous poursuivons nos travaux sur l'actualisation de la revue nationale stratégique (RNS) 2022 par l'audition de Mme Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique.

Le cyber et l'intelligence artificielle (IA) sont des domaines fondamentalement duaux, à la croisée du civil et du militaire. Les innovations du premier alimentent le second. Le ministère des armées s'est engagé dans une stratégie d'intégration des innovations et des développements issus du secteur civil, notamment depuis la création de l'Agence ministérielle pour l'intelligence artificielle de défense (Amiad), dont nous avons auditionné le directeur, M. Rondepierre, le 29 janvier.

La rapidité des évolutions technologiques dans le secteur civil constitue un défi d'envergure pour la défense nationale. De la sophistication des cyberattaques, notamment grâce à l'IA, à l'essor des fausses informations dans le champ informationnel, nos armées doivent sans cesse s'adapter pour faire face à des menaces protéiformes, qui naissent souvent dans le secteur civil. Ces évolutions technologiques sont aussi porteuses d'opportunités pour nos armées, qui peuvent en tirer des avantages opérationnels décisifs sur le champ de bataille.

La RNS consacre une place importante à la cyberdéfense, notamment à la résilience cyber de la nation, qui est l'objectif stratégique (OS) n° 4. L'IA, en revanche, ne fait pas l'objet d'un développement particulier. Son actualisation sera sans doute l'occasion d'y remédier. Dans ce contexte, votre connaissance de l'IA et des enjeux cyber est particulièrement utile.

Mme Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique. Je vous remercie de m'avoir invitée à m'exprimer devant votre commission pour évoquer, dans le cadre de l'actualisation de la RNS, les enjeux et les défis immenses auxquels est confronté notre pays en matière de réponse à la menace et de renforcement de notre sécurité dans les domaines du cyber de l'IA. Plusieurs administrations attachées à l'utilisation du numérique dans l'environnement de défense participent à cette réflexion sous la tutelle de mon collègue Sébastien Lecornu, notamment le secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (Anssi) et la direction générale des entreprises (DGE). L'engagement et la qualité des travaux de votre commission sont un atout précieux pour le renforcement de notre sécurité.

Je prends la parole devant vous, compte tenu du contexte que nous connaissons, avec une certaine gravité, mais aussi avec confiance dans notre réponse collective. Les menaces se multiplient, se transforment et s'intensifient, mais nous avons toujours su, et nous savons encore, bâtir des réponses solides et cohérentes, et sommes en capacité d'aller toujours plus loin. Nous avons veillé à conserver ou à acquérir la maîtrise des technologies ayant un impact sur notre souveraineté. Nous l'avons fait en construisant un modèle de dissuasion indépendant, en faisant du nucléaire une source d'énergie prépondérante et en développant une industrie de défense cohérente et robuste. Nous nous employons désormais à faire de même pour le numérique, notamment dans les domaines de la cybersécurité et de l'IA, devenus des pièces maîtresses dont notre architecture de sécurité et nos plans doivent tenir compte.

Des exemples toujours plus nombreux le démontrent. Une vulnérabilité numérique peut, en quelques heures, neutraliser une entreprise, une collectivité, un hôpital, une infrastructure stratégique, et potentiellement paralyser une région, voire un pays, jusque dans le fonctionnement de son système démocratique. Ces enjeux doivent être pris en considération avec sérieux et détermination pour être à la hauteur les défis auxquels nous sommes confrontés, et qui s'intensifieront dans les années à venir.

Récemment encore, nous étions essentiellement confrontés à une menace de nature physique. Depuis quelques années, nous devons engager des actions pour répondre à une menace hybride. Nous avons été précurseurs et nous ne partons pas de rien. Dès 2006, la France a mis en œuvre le dispositif Secteur d'activité d'importance vitale (SAIV) visant à lutter contre les risques auxquels sont exposées les infrastructures des opérateurs d'importance vitale (OIV). Ce cadre a permis de sécuriser les infrastructures critiques face aux menaces terroristes, industrielles, environnementales et numériques.

Je salue le travail accompli dans le cadre de l'élaboration de la RNS 2022. Ce document nous a permis de tracer une ligne claire : celle d'une souveraineté retrouvée et de l'autonomie de notre capacité d'appréciation, de décision et d'action. La RNS 2022 a posé les fondements d'un renforcement de notre outil militaire, d'une modernisation de nos capacités, d'une consolidation de notre posture cyber et de l'affirmation de notre ambition européenne. Elle a répondu au besoin de clarifier notre doctrine, de hiérarchiser nos efforts et de donner un cap à nos services, à nos forces et à nos industriels.

Elle s'est concrétisée dans le cadre de la loi de programmation militaire (LPM) 2024-2030, qui a joué un rôle déterminant en dotant nos forces et nos administrations des moyens nécessaires pour renforcer notre sécurité. Outre un effort budgétaire inédit, elle offre une vision intégrée des menaces rassemblant la dissuasion nucléaire, la conflictualité hybride, la résilience nationale et les nouveaux champs stratégiques du cyber et de la lutte informationnelle.

Nous devons désormais aller plus loin. Le monde a changé. La menace change en permanence de nature, d'échelle et de rythme. Elle est devenue hybride, mêlant les actions physiques, cyber, informationnelles et économiques. Le numérique en est le cœur. L'OS n° 9 de la RNS illustre parfaitement cette mutation, en affirmant la nécessité de lutter dans les champs de l'hybridité en conjuguant nos efforts dans les champs du cyber, de la guerre informationnelle, de la guerre cognitive et des stratégies d'influence.

L'essor de l'IA et l'intensification des tensions géopolitiques renforcent la nécessité de nous adapter. Depuis la publication de la RNS 2022 il y a trois ans, nous assistons à une double transformation du paysage stratégique mondial.

La première est due à l'essor fulgurant de l'IA générative, à la généralisation des modèles de langage, à la démocratisation des usages et à la montée en puissance des applications civiles et militaires de l'IA. L'IA est un catalyseur de puissance, un levier de domination, notamment économique, et un facteur de déséquilibre. Elles offrent des gains opérationnels inédits, notamment dans le renseignement, la simulation, la logistique et la conduite des opérations. Elle ouvre la voie à de nouvelles vulnérabilités, liées à l'opacité des algorithmes, au risque d'empoisonnement des données d'entraînement des modèles, à la dépendance technologique, aux asymétries cognitives et à la manipulation de l'information.

Elle est d'ores et déjà utilisée à des fins de déstabilisation, sous la forme de deepfakes simulant des messages diplomatiques, de faux documents générés par des IA circulant dans les médias, notamment en période électorale, comme ce fut le cas récemment chez certains de nos voisins, et de voix artificielles imitant celles de responsables publics. Cette guerre informationnelle fondée sur la simulation nous met à l'épreuve ; elle met notamment à l'épreuve notre capacité collective à discerner le faux du vrai.

La seconde transformation est l'intensification des tensions géopolitiques. La Russie mène une confrontation hybride globale. La Chine articule sa puissance technologique et sa stratégie d'influence. D'autres puissances, qui ne sont pas toutes des États, exploitent notre cyberespace pour y mener des actions offensives dans une logique de déstabilisation, de sabotage, d'intimidation et d'espionnage. En 2024, l'Anssi a enregistré une croissance de 15 % des cyberattaques, qui visent les entités de toute nature. Réussies, elles peuvent mettre à l'arrêt une activité pendant plusieurs semaines – je l'ai constaté dans des hôpitaux et des collectivités locales qui en ont subies, rendues incapables de poursuivre leur activité, touchées de plein fouet par les tensions géopolitiques.

Des campagnes de désinformation ciblées ont été détectées. Elles cherchent à affaiblir notre parole, à diviser, à propager le doute dans l'opinion. Elles visent, par des moyens numériques, à affaiblir la crédibilité de l'État et des représentants de la nation ainsi que la confiance que leur portent les citoyens. Nos sociétés démocratiques sont particulièrement exposées et mises à l'épreuve par ces pratiques de désinformation redoutablement efficaces.

Ces évolutions ont amené le Président de la République à faire réviser la RNS 2022. Ce travail nécessaire et urgent vise à fonder sur un diagnostic précis une ambition à la hauteur des enjeux et proposer des leviers opérationnels permettant une mise en œuvre efficace. À ce titre, votre expertise, éclairée par les auditions que vous avez menées, sera précieuse. S'agissant du numérique et des plans structurants pour la cybersécurité, l'IA et la lutte contre la désinformation me semblent être des piliers fondamentaux pour notre avenir.

En matière de cybersécurité, les attaques sont de plus en plus nombreuses, mais aussi de plus en plus sophistiquées, variées et automatisées. Surtout, elles touchent un public toujours plus large. Elles ne visent plus seulement les grandes structures. Les entités de toute nature y sont confrontées. Nous devons développer nos propres capacités de défense et protéger nos infrastructures stratégiques, nos entreprises, nos collectivités et nos citoyens face aux nouvelles formes de menace.

Tel est l'objet du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, adopté par le Sénat le 12 mars, que je présenterai devant votre assemblée dans quelques mois. Il s'articule autour de trois axes.

Le titre I vise à transposer la directive sur la résilience des entités critiques, dite REC, ce qui permettra d'élargir le périmètre du dispositif précurseur qu'est la sécurité des activités d'importance vitale (SAIV), et de basculer dans une logique de résilience fondée sur le triptyque anticiper – résister – se rétablir. La question n'est plus de savoir si mais quand une attaque aura lieu. Les entités doivent en avoir conscience. La directive REC inclut des secteurs supplémentaires dans les infrastructures critiques, notamment l'assainissement, les

réseaux de chaleur et l'hydrogène. Il s'agit de faire basculer les opérateurs dans une logique de protection physique et hybride, et de résilience.

Le titre II vise à transposer la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite NIS2, négociée pendant la présidence française du Conseil de l'Union européenne (PFUE). Il s'agit de changer d'échelle dans le renforcement de notre cybersécurité collective, face à une menace de plus en plus diffuse. La directive couvre 15 000 entités, contre 500 pour la précédente, opérant dans dix-huit secteurs d'activité essentiels à la confiance de nos concitoyens dans les institutions et à la sécurité de leur quotidien, tels que l'eau, l'agroalimentaire, la gestion des déchets et l'énergie.

La directive NIS2 distingue deux types d'entités, afin d'assurer la progressivité des obligations. Les entités importantes seront soumises à des obligations de base en matière cyber, visant à s'assurer qu'elles ne seront pas paralysées par le premier rançongiciel venu. Les entités essentielles en raison de leur secteur d'activité, de leur taille, de leur chiffre d'affaires, de la criticité de leur activité et de leur exposition à des menaces plus sophistiquées devront respecter des exigences accrues et se prêter à des contrôles en amont et en aval pour s'assurer qu'elles sont prêtes à faire face aux menaces.

Le titre III vise à transposer la directive sur la résilience opérationnelle numérique du secteur financier, dite DORA. Particulièrement vulnérable, le secteur financier a été la cible de plus de 20 millions d'attaques au cours des vingt dernières années ; les pertes s'élèvent à plusieurs centaines de millions.

Je retire de mes rencontres sur le terrain un enseignement essentiel : la question de la cybersécurité n'est plus cantonnée aux experts et aux grandes structures. Toute entité, de la petite à la grande entreprise en passant par la collectivité locale, peut être touchée. Il faut ancrer une culture partagée dans tous les territoires et à tous les niveaux de responsabilité.

Tel est l'objet du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Un véritable effort de formation, de sensibilisation et d'accessibilité à des ressources techniques et humaines s'impose pour contrer la menace cyber. Je serai très attentive à la bonne application de la loi, s'agissant notamment de l'accompagnement des structures dans la mise en œuvre des règles de conformité et de la sensibilisation.

J'en viens à plusieurs axes de réflexion ne relevant pas directement de mon ministère, la cybersécurité étant par nature transversale, et sa gouvernance interministérielle.

Dès lors que la directive NIS2 fait passer de 500 à 15 000 le nombre d'entités couvertes, elle soulève la question des moyens pour faire passer à l'échelle notre nation et notre cybersécurité collective. La mise en œuvre de cet indispensable levier réglementaire fait naître un fort besoin d'accompagnement, notamment des entités les moins matures – j'en ai nettement conscience pour les avoir rencontrées –, pour lesquelles la mise en conformité est parfois une marche élevée. Tel est le cas des collectivités, des hôpitaux – auxquels est dédié le programme Cybersécurité accélération et résilience des établissements (Care) –, des petites et moyennes entreprises (PME) et des entreprises de taille intermédiaire (ETI), qui ne sont pas toujours outillés sur les plans humain, technique et méthodologique pour franchir la marche de la conformité en pleine autonomie.

Nous ne partons pas de rien. Dans le cadre du plan France relance et du programme Care, l'Anssi, dont les parcours cyber ont eu des effets très positifs, a accompagné plus de 1 000 entités publiques, qui disposent désormais d'un socle de cyberrésilience commun. Ces parcours n'ont pas été dimensionnés pour couvrir les 15 000 structures visées par la directive NIS 2, ce qui au demeurant n'est pas souhaitable : à l'heure où le risque cyber va croissant, il importe que les entités prennent la responsabilité de leur cybersécurité dans la gestion de leurs budgets.

Cela n'exclut pas d'envisager de prendre des mesures complémentaires, notamment pour les collectivités et les universités, visées en 2024 par des attaques en nombre croissant. Il s'agit de densifier, renforcer et coordonner le travail réalisé par les formidables et nombreux acteurs de l'accompagnement cyber dans les territoires, tels que le groupement d'intérêt public (GIP) Action contre la cybermalveillance, les campus régionaux de cybersécurité et de confiance numérique, les centres de réponse aux incidents de cybersécurité (CSIRT) et le commandement de la cyberdéfense (Comcyber). La dynamique du réseau des treize Csirt est très positive. Lancé il y a à peine un an, il mériterait d'être renforcé tant il joue un rôle fondamental dans l'accompagnement de terrain, indispensable à l'application du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

La deuxième question transversale que je souhaite évoquer est celle des moyens de l'Anssi, qui sont en augmentation continue depuis 2022. Vous en décidez ainsi chaque année lors de l'examen du projet de loi de finances. Cette hausse devrait se poursuivre jusqu'en 2027, ce qui est une très bonne chose.

L'Anssi remplit ses missions au plus près du terrain. Elle est reconnue par tous ses interlocuteurs, notamment dans le cadre de la directive NIS2, comme un accompagnateur important. Elle a démontré son expertise technique en matière de menace cyber lors de la préparation des Jeux olympiques et paralympiques (JOP) de Paris 2024. Sa réputation à l'international est excellente.

Avec trois fois moins d'équivalents temps plein (ETP) que son homologue allemande, elle n'est pas trois fois moins efficace, au contraire. Elle pallie cette différence de moyens par sa performance et par la spécificité de son modèle, qui fait d'elle un chef de file qui engage et coordonne des moyens concrets en propre et par l'intermédiaire de nombreux relais démultipliant son action, au premier rang desquels les prestataires de services qualifiés. Il n'en reste pas moins que, compte tenu du contexte géopolitique et de l'intensification structurelle de la menace, qui pourraient aggraver la tension à laquelle sont d'ores et déjà soumis nos moyens collectifs, nous pouvons nous demander quelle trajectoire adopter pour maintenir notre niveau d'exigence.

Le troisième axe de réflexion est notre potentiel d'innovation. Pour éviter la dépendance technologique, nous devons préserver notre capacité à maîtriser les technologies cyber critiques. L'écosystème national est robuste et dynamique, ce qui est un impératif majeur pour assurer notre autonomie stratégique, d'autant que la technologie évolue très rapidement, et fournir des solutions souveraines aux organisations qui doivent se sécuriser. Faire en sorte que ces entités disposent de solutions françaises ou européennes, et par là même faire croître l'écosystème cyber français, doit être un objectif collectif.

Grâce à la stratégie cyber de France 2030 et à l'excellence de nos entreprises ainsi que de nos industriels, nous sommes très bien positionnés sur plusieurs segments tels que l'analyse de la menace, la détection et la cryptographie post-quantique. Nous avons des pépites très prometteuses ayant le potentiel de devenir des champions européens.

Nous devons continuer à consolider notre écosystème, à les accompagner et à les soutenir. Le meilleur moyen pour ce faire est de passer commande auprès d'elles et d'inciter nos entreprises à faire de même, en améliorant leur accès à la commande publique et aux contrats à tous les stades du développement, en intégrant mieux les offres innovantes dans les politiques d'achat public et privé, et en renforçant notre capacité collective à les projeter à l'international grâce à l'export.

En matière d'IA, nous n'avons pas attendu la RNS 2022 pour nous mettre en ordre de marche. La stratégie nationale pour l'intelligence artificielle figure dans la RNS 2018. Voulue par le Président de la République, elle nous a permis d'avoir une longueur d'avance. Nous avons investi 2,5 milliards pour construire des technologies d'IA souveraines, souvent à potentiel dual, financer nos infrastructures et former des talents de haut niveau, qui sont à mes yeux notre atout maître dans la course à l'IA.

Nous avons mis l'accent sur le développement de l'IA embarquée et de l'IA de confiance. Depuis quelques années, nous avons pris le virage de l'IA générative, qui révolutionne tous les secteurs de la défense. Ces investissements se poursuivent, en donnant la priorité à l'IA embarquée et à la robotique.

Par ailleurs, nous œuvrons au renforcement de nos infrastructures critiques indispensables à une IA souveraine et européenne, au premier rang desquelles des infrastructures publiques de calcul nécessaires à l'entraînement des modèles. En la matière, nous avons été pionniers en mettant à la disposition de nos chercheurs le calculateur Jean Zay. Le supercalculateur Alice Recoque, qui a reçu le label européen il y a deux semaines, nous permettra de poursuivre cet effort.

Des infrastructures privées complètent ces infrastructures publiques. À l'occasion du Sommet pour l'action sur l'IA, le Président de la République a annoncé 109 milliards d'investissements pour financer de nouveaux calculateurs sur le sol français. MistralAI, l'une de nos pépites, se dotera de sa propre infrastructure de calcul.

Par ailleurs, nous souhaitons renforcer notre atout maître que sont les talents. Neuf centres d'excellence, partout sur le territoire, formeront 100 000 personnes en IA d'ici 2030. L'Amiad œuvre aussi à la formation avec un effectif de 130 experts de très haut niveau, qu'il est prévu de porter à 250 personnes d'ici la fin de l'année.

Ces trois piliers – talents, infrastructures, R&D – seront renforcés grâce aux 400 millions annoncés lors du Sommet pour l'action sur l'IA pour financer un pilier national de notre stratégie. Nous les allouerons au mieux en tenant compte du contexte.

S'agissant du *cloud*, qui est l'un des domaines les plus stratégiques pour la souveraineté de nos données, la réflexion sur la réduction de notre dépendance s'impose. Elle doit être menée à l'échelle européenne. La France a constamment rappelé avec force la nécessité de se doter d'une capacité de cloud souverain et de protection de nos données au

plus haut niveau à l'échelle de l'Union européenne. Nous avons été pionniers en introduisant la qualification SecNumCloud. Nous continuerons à défendre cette ambition.

Outre les attaques cyber et l'IA, ce qui nous menace, c'est la guerre informationnelle et l'impact des plateformes numériques et des réseaux sociaux sur notre démocratie, dont certains sont devenus des vecteurs majeurs d'influence exposant nos citoyens à des campagnes de désinformation, de manipulation et d'ingérence. La préservation de notre cohésion sociale et démocratique, qui nous semblait acquise, est devenue, à l'heure des réseaux sociaux, une question qu'il est urgent de mettre sur la table, pour nous comme pour nos voisins européens. Les récentes tentatives d'ingérence en Roumanie démontrent que la menace est bien réelle. Il faut y faire face de façon transnationale et coordonnée à l'échelon européen.

Tel est l'objet du règlement relatif à un marché unique des services numériques (DSA) et du règlement relatif aux marchés contestables et équitables dans le secteur numérique (DMA), qui imposent aux plateformes des obligations accrues en matière de transparence et de responsabilité s'agissant des contenus illicites, qui ne le sont pas moins parce qu'ils sont en ligne, et de la manipulation de l'information. Ils offrent une première base solide pour lutter contre les ingérences étrangères et protéger l'intégrité de notre débat public. La France veillera à leur bonne application à l'échelon européen.

Nous nous sommes dotés d'un service dédié à la lutte contre les ingérences étrangères et la manipulation de l'information, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), que toute l'Europe nous envie. Lors de la réunion ministérielle informelle des télécommunications du Conseil européen qui s'est tenue au début du mois et qui était, pour la première fois, entièrement consacrée à l'IA, Viginum a été cité pour sa qualité. La présidente de la Commission européenne souhaite que ce modèle soit répliqué dans les autres États membres en vue de constituer un réseau.

L'actualité récente démontre qu'un effort supplémentaire est nécessaire en matière de lutte contre la manipulation de l'information et les ingérences étrangères. La révision de la RNS doit nous permettre d'ouvrir le débat des moyens alloués à ces priorités, à l'heure où la France et l'Union européenne font face à une nouvelle forme de conflit informationnel et cyber.

Ce combat pour notre souveraineté numérique et pour la sécurité de nos concitoyens doit inclure les chercheurs, les ingénieurs, les enseignants, les élus locaux et les citoyens en général. L'enjeu est de faire naître une culture de la défense et de la souveraineté numériques, qui me semble nécessaire pour être à la hauteur des enjeux et de la menace cyber. J'appelle à la résilience collective. Tel est le sens de l'engagement du gouvernement.

M. le président Jean-Michel Jacques. Nous en venons aux interventions des orateurs des groupes.

M. Frank Giletti (RN). L'IA est une technologie de rupture. L'histoire militaire enseigne que l'adoption tardive d'une innovation décisive peut être un facteur de déclassement. Le ministère des armées prend de nombreuses initiatives, ce dont le groupe Rassemblement national se réjouit.

L'articulation entre le civil et le militaire est une question centrale. Dans le domaine de l'IA, l'innovation est le fait du secteur privé, souvent d'acteurs non traditionnels de la défense. Aux États-Unis, des entreprises telles que Shield AI ou Anduril développent des solutions de combat autonomes en rupture avec les approches classiques, en investissant massivement dans des logiciels avancés.

En France et en Europe, si notre modèle repose encore largement sur les grands industriels de défense historiques, des entreprises privées telles que Helsing proposent aussi des solutions. Votre ministère et Bercy sont-ils prêts à aider à leur financement, dans une course mondiale où chaque année compte ?

S'agissant de notre souveraineté technologique, nos armées doivent tirer parti des avancées de l'IA tout en évitant de dépendre excessivement des géants du numérique étrangers. L'hégémonie des Gafam et l'émergence de standards internationaux imposés hors du cadre étatique font courir un risque à notre autonomie stratégique. Quelle part de notre souveraineté devons-nous préserver ? Avec quels garde-fous ?

Outre ces enjeux industriels et stratégiques, l'intégration de l'IA dans nos systèmes de défense soulève une question déterminante : celle de notre dissuasion nucléaire, dont la crédibilité repose sur la maîtrise humaine absolue de la décision ultime. L'autonomisation croissante des systèmes d'armes ne risque-t-elle pas d'altérer tôt ou tard ce principe fondamental ? Quelle est la doctrine du gouvernement en la matière ?

L'IA renforce la surveillance spatiale, en anticipant tirs et trajectoires. Certains compétiteurs l'exploitent pour le combat, le brouillage et l'interception. Qu'entreprend la France de son côté ? L'Europe envisage de se doter d'une constellation de satellites en orbite basse ne dépendant pas des États-Unis et recourant à l'IA pour la surveillance et le ciblage, complémentaire de nos capacités patrimoniales. Comment soutenir cette initiative et en accélérer le développement ?

Mme Clara Chappaz, ministre déléguée. S'agissant du financement de l'innovation privée, Éric Lombard a annoncé la semaine dernière le lancement du plan de financement de l'économie de défense. La Banque publique d'investissement (BPIFrance) a annoncé la création d'un fonds dédié à l'innovation de défense. Nous sommes pleinement mobilisés pour que les sociétés de notre écosystème, qui est assez vigoureux, soient au centre de l'innovation de défense et financièrement soutenues. Concrètement, nous organisons des rencontres entre les entreprises innovantes de la DefTech, BPIFrance et des financeurs privés.

Nous avons évoqué le renforcement des partenariats public-privé (PPP) lors de la réunion ministérielle informelle des télécommunications du Conseil européen qui s'est tenue à Varsovie au début du mois. Lors de la PFUE, il avait été envisagé de créer, dans le cadre du règlement européen sur la cybersécurité, une réserve cyber. Nous avons relancé l'idée à Varsovie.

L'objectif est clair : renforcer la collaboration entre civils et militaires en matière de cybersécurité pour labéliser des acteurs privés à l'échelle de l'Union européenne – nous soutiendrons les acteurs français pour qu'ils bénéficient de ce programme – ayant vocation à venir en aide à l'écosystème public et aux administrations européennes en cas de cyberattaque majeure. L'appel à projets sera lancé cet été, pour un budget de 30 millions. Il ne s'agit pas de financer des solutions, mais de mobiliser et de renforcer les PPP que le président de la

République a appelé de ses vœux en 2022. L'écosystème cyber a accueilli favorablement cette initiative.

S'agissant de la souveraineté, la dépendance de l'Europe à certains acteurs, pour certaines technologies de la chaîne d'infrastructures numériques, est bien réelle. La création du référentiel SecNumCloud par l'Anssi fonde une doctrine très claire en matière de souveraineté des données, visant à nous assurer que les données les plus sensibles de Françaises et des Français sont stockées dans un cloud souverain, d'une part, et, d'autre part, et à encourager la montée en puissance d'une offre française et européenne. Notre politique a toujours marché sur deux jambes, la sécurisation et le soutien à l'écosystème d'innovation privée pour qu'il offre des solutions adaptées à l'augmentation des besoins de sécurisation. Tel est l'objet des doctrines SecNumCloud et « Cloud au centre ».

Ce sujet est éminemment européen. La position de la France est claire et inchangée au fil des ans – mes prédécesseurs ont consacré beaucoup de temps et d'énergie à la faire valoir. Le contexte géopolitique incite à rouvrir ces conversations à l'échelon européen, comme nous l'avons fait à Varsovie.

Les retards technologiques pèsent non seulement sur la souveraineté et sur la sécurité, mais aussi sur l'économie du continent. Comme l'a montré le rapport Draghi, l'investissement dans les technologies vise non seulement à renforcer notre sécurité, mais aussi à combler notre retard de compétitivité.

S'agissant de l'évolution de notre dissuasion, il ne m'appartient pas, en tant que ministre déléguée chargée de l'intelligence artificielle et du numérique, de la commenter. Je transmettrai vos questions à mon collègue Sébastien Lecornu.

Mme Emmanuelle Hoffman (EPR). La France a fait de l'IA une priorité stratégique. Se saisir des enjeux de l'IA dans le domaine de la défense est indispensable pour garantir souveraineté et sécurité. Face à la rapidité des avancées technologiques et à une compétition internationale accrue, notre pays ne peut pas se permettre de prendre du retard. Votre engagement et celui du ministre des armées témoignent de l'importance accordée à ce sujet au plus haut niveau de l'État.

Le gouvernement a défini une stratégie nationale ambitieuse. D'ici 2030, 2 milliards seront consacrés au développement de l'IA de défense. Depuis 2018, 2,5 milliards ont été investis dans la recherche et la technologie. Grâce à des efforts remarquables, neuf pôles d'excellence ont été créés et la capacité du supercalculateur Jean Zay a été étendue. En 2024, la création de l'Amiad a été une étape cruciale dans la centralisation et l'accélération de nos efforts en matière d'IA militaire.

Ces avancées significatives n'effacent pas les défis majeurs. Les États-Unis et la Chine investissent respectivement 200 et 150 milliards dans l'IA militaire, creusant un écart considérable avec nos moyens. Notre dépendance technologique, notamment en matière de semi-conducteurs et d'infrastructures de calcul, telles que les processeurs graphiques de Nvidia, est préoccupante.

Face aux investissements massifs des États-Unis et de la Chine, comment la France compte-t-elle réduire l'écart technologique tout en préservant son indépendance ? Quelle stratégie adopter pour tirer parti de la dualité entre les applications civiles et militaires ?

Quelles mesures sont prises pour garantir une infrastructure souveraine, renforcer notre écosystème d'innovation et surtout attirer et conserver nos talents ?

Mme Clara Chappaz, ministre déléguée. L'IA est un sujet interministériel. Lors du Sommet pour l'action sur l'IA, accueilli en France autour du premier ministre, un comité interministériel de l'IA pour, dans tous les ministères – celui des armées est très en avance –, passer en revue les feuilles de route et en accélérer le déploiement, pour qu'ils se saisissent pleinement de cette technologie.

La stratégie ministérielle pour l'IA de défense repose notamment sur quinze centres de la donnée et de l'IA, placés au plus près des opérationnels, et sur l'Amiad, dont l'objectif est de déployer des cas d'usage de l'IA dans le domaine de la défense et des infrastructures de calcul, dont les capacités permettent de spécialiser et d'entraîner les modèles d'IA de défense.

Un supercalculateur classifié, le plus grand d'Europe, sera livré à l'automne 2025 et installé au Mont Valérien. Il permettra à la France de traiter les données confidentielles et de tirer pleinement profit de l'IA au bénéfice des armées et des entreprises de défense. Souverain et non connecté, sa maintenance sera assurée par des personnels habilités au secret de la défense nationale, ce qui permettra de mettre à la disposition de notre industrie de défense tout le potentiel de l'IA. Par ailleurs, à moyen et à long terme, le ministère des armées lance un plan de politique industrielle en collaboration avec les acteurs de la recherche, de l'innovation et de l'industrie.

S'agissant de notre souveraineté et des dépendances, nous avons un atout dans la course à l'IA : une électricité abondante et décarbonée, issue du nucléaire. Contrairement au reste de l'Europe, notamment à l'Allemagne, nous pouvons accueillir une capacité de calcul importante, nécessaire au développement des modèles d'IA les plus performants. Les 109 milliards annoncés lors du Sommet pour l'action sur l'IA sont un véritable atout compétitif, le développement de l'IA reposant sur l'accès aux capacités de calcul nécessaires à l'entraînement des modèles. Nous avons démontré que nous sommes dans la course. La France, grâce à son offre énergétique et à son écosystème de recherche, est attractive.

Concernant les puces et les semi-conducteurs, nous sommes très dépendants des pays étrangers, qu'il s'agisse de l'extraction des matières premières, notamment des terres rares, ou de la production des composants. Nvidia jouit d'un quasi-monopole. Dans le contexte géopolitique actuel, nous sommes exposés à des changements d'attitude potentiels des autorités américaines. La France figure toujours sur la liste des pays qui peuvent s'approvisionner en puces.

Mes homologues européens et moi-même suivons de très près la situation, conscients de l'impact qu'auraient des pénuries dans ce domaine dès lors qu'il n'existe aucune autre solution pérenne. En outre, la moitié de la production mondiale de semi-conducteurs dépend d'une entreprise taïwanaise. Nous avons lancé un appel à projets la semaine dernière pour renforcer la collaboration avec Taïwan sur l'aval de la chaîne de valeur.

Dans le domaine du cloud, le label cloud de confiance complète la stratégie « Cloud au centre ». La transformation numérique est indispensable pour renforcer la compétitivité de nos entreprises et de nos administrations et moderniser nos services publics. À l'aune de la protection des données sensibles, de la souveraineté numérique et de l'enjeu économique, il n'est pas inutile de rappeler que les fournisseurs européens ne représentent que 13 % du

marché du cloud. Nous devons continuer à faire avancer une stratégie sur deux jambes : adopter des référentiels de sécurisation de la donnée et soutenir, grâce à des appels à projets dédiés, la montée en puissance et en compétence de nos offres de cloud pour associer à la politique de sécurité une politique industrielle.

S'agissant des talents, ils sont fondamentaux dans toutes les technologies. Ils forment le deuxième pilier de la stratégie nationale pour l'intelligence artificielle, dans laquelle 2,5 milliards ont été investis depuis 2018. Nous l'avons renforcé lors du Sommet pour l'action sur l'intelligence artificielle, en annonçant un effort de 360 millions pour soutenir la montée en puissance des neuf centres d'excellence répartis sur le territoire. L'objectif est de former 100 000 talents en IA, à tous les degrés de formation.

L'excellence scientifique française est reconnue dans le monde entier, notamment en mathématiques. La France est classée troisième au classement de Shanghai. Nous disposons des meilleurs experts en IA. Nous devons non seulement renforcer nos formations d'excellence, mais aussi déployer une stratégie de massification des talents, parce que les usages de l'IA sont partout.

M. Aurélien Saintoul (LFI-NFP). Nous sommes tous d'accord pour contresigner vos objectifs en matière de souveraineté et de conservation des talents, mais de nombreux exemples indiquent que les objectifs ne sont pas atteints et les pétitions de principe pas toujours suivies d'effets. Nous avons appris récemment que l'éducation nationale confie à Microsoft le soin d'administrer ses données. Pour son supercalculateur, l'Amiad a fait appel à HP pour son supercalculateur plutôt qu'à Atos. La restructuration de la dette de cette dernière aboutira à une vente à la découpe de l'entreprise, alors même que l'on voit mal comment mettre en œuvre une stratégie ambitieuse en matière de données sans elle.

Un an et demi après son entrée en vigueur, pouvez-vous dresser un bilan du règlement européen sur les semi-conducteurs ? Des investissements ont-ils été réalisés ? A-t-il fait sortir de terre quelque chose ?

Concernant les plateformes, est-il envisageable d'entrer dans un rapport de force avec M. Musk, manifestement devenu un acteur de déstabilisation de l'Europe, sans attendre l'entrée en vigueur du code de conduite intégré au règlement européen sur les services numériques (DSA), dont il n'est pas certain au demeurant qu'il permette de le sanctionner ? Sommes-nous obligés d'attendre que Bruxelles se mobilise pour faire respecter ce que la France considère comme des obligations en matière de respect du débat public ?

Mme Clara Chappaz, ministre déléguée. L'éducation nationale a renouvelé pour quatre ans l'accord-cadre conclu avec Microsoft en 2020. Il offre un support juridique permettant à l'administration de continuer à utiliser les logiciels de la suite Microsoft qui équipent ses ordinateurs, en renouvelant les licences à un tarif préférentiel, sans minimum d'achat. Tous les ministères ont conclu un tel accord. Celui conclu par le ministère de l'éducation nationale porte sur un montant très élevé, car plusieurs millions de postes sont concernés. Par ailleurs, son périmètre a été élargi aux organismes de recherche et aux universités pour réaliser des économies d'échelle.

Cet accord-cadre ne modifie en rien la doctrine « Cloud au centre ». La partie du contrat relative au stockage des données est réduite. Les données sensibles du ministère, nonobstant le montant du contrant, demeurent stockées dans des serveurs internes hébergés en

France, conformément à la circulaire signée par Élisabeth Borne en 2023. Seules les données qui ne sont pas sensibles peuvent être hébergées dans des clouds commerciaux.

Les questions que vous soulevez méritent toutefois d'être posées. Notre doctrine est claire : toute donnée sensible doit être stockée dans un cloud certifié SecNumCloud pour en garantir la confidentialité. Dans le cas de Microsoft, seuls les logiciels sont concernés.

La direction interministérielle du numérique (Dinum) travaille au déploiement de logiciels offrant une solution alternative à Windows, mais le fait est que nous sommes dépendants de cette suite logicielle. La sécurisation et la montée en puissance de solutions alternatives sont un préalable à la sortie de cette dépendance. Le travail sur le futur environnement de travail numérique de l'agent public commence à porter ses fruits. L'usage de nouveaux outils de communication instantanée et de travail collaboratif se répand, mais la solution à ce problème se construira dans la durée, dans le cadre du renforcement continu d'une politique publique numérique.

S'agissant du cloud, nous faisons monter en puissance des solutions alternatives. Nous réaffirmons la doctrine énoncée par Élisabeth Borne en 2023, visant à s'assurer que les processus d'utilisation des données sont compris et respectés. La sécurité de nos données est un sujet sensible et d'actualité, appelant un renforcement de la communication et de l'accompagnement des ministères.

Le règlement européen sur les semi-conducteurs vise à préserver la position de l'Europe dans le domaine des semi-conducteurs, en apportant un soutien massif à des projets européens, en assurant la souveraineté de la chaîne de valeur. Nous travaillons à l'identification des limites, au premier rang desquelles la durée des procédures, notamment des projets d'intérêt européen commun (Piec), et l'attractivité de l'écosystème de financement et du territoire européens – Intel et Wolfspeed ont renoncé à leurs projets.

Des évolutions du règlement européen sur les semi-conducteurs sont envisagées pour tenir compte de la transformation de notre environnement, caractérisée notamment par la montée en puissance des composants pour l'IA qui renforce notre dépendance, la dégradation de l'industrie, les mesures de contrôle des exportations américaines et l'incertitude géopolitique ainsi que, s'agissant des États-Unis, commerciale.

La Commission européenne a dressé un premier bilan du règlement européen sur les semi-conducteurs et réfléchit aux orientations à suivre pour insuffler une nouvelle dynamique, visant notamment à susciter une coopération européenne en la matière, à l'initiative des Pays-Bas. Comme l'indique le rapport Draghi, une véritable politique européenne en matière de semi-conducteurs exige de préciser et de hiérarchiser nos objectifs.

Mme Marie Récalde (SOC). Certains chercheurs affirment que la France s'autorise à développer des systèmes d'armes létales autonomes (Sala), au motif qu'il y aura toujours un humain dans la boucle. Est-ce le cas ? Quelles sont les recommandations du Comité d'éthique de la défense sur ce point ?

S'agissant de notre participation aux structures de résilience cyber européennes, l'Objectif stratégique n° 6 de la RNS fait de la France l'un des moteurs de l'autonomie stratégique européenne, destinée à jouer un rôle majeur dans le cadre d'une complémentarité accrue et durable entre l'Union européenne et l'Otan. Comment évaluez-vous le niveau de

coopération dans le domaine du cyber avec l'Otan en Europe ? Quel rôle la France joue-t-elle dans ce système ?

Mme Pouzyreff et moi-même menons actuellement une mission d'information sur l'opérationnalisation de la nouvelle fonction stratégique "influence", qui s'inscrit dans la révision de l'OS n° 9 de la RNS. Nous travaillons notamment sur la guerre cognitive. Comment envisagez-vous la lutte contre ces stratégies insidieuses visant à saper les fondements de notre société et à éroder à long terme notre cohésion nationale ? Les sciences cognitives sont-elles suffisamment mobilisées par l'État ? Ne faudrait-il pas, dans la RNS, renforcer nos stratégies défensives par des stratégies offensives ?

Mme Clara Chappaz, ministre déléguée. Ayant oublié de répondre à la question de savoir si nous ferons en sorte que le DSA soit respecté par les propriétaires des plateformes, je commencerai par dire que tel sera le cas. Nous avons rappelé à la Commission, en Européens, notre attachement vigilant à la bonne application du DSA. Il est fondamental que les enquêtes qui les visent à l'échelon européen soient menées à bien, en prenant le temps nécessaire pour qu'elles soient solides, étant donné qu'elles seront sans doute contestées. Les États membres – j'étais ce matin avec mon homologue danoise – sont nombreux à avoir rappelé leur attachement au respect de ce cadre.

Les plateformes ont un rôle important à jouer dans la lutte contre la manipulation de l'information. Le DSA, texte ambitieux et adopté de façon transpartisane, leur en attribue la responsabilité. Contrairement à ce que l'on entend dire, ni la Commission européenne ni un État membre ne peut décider de la véracité de tel ou tel contenu. Il s'agit seulement de rendre les plateformes responsables des contenus qu'elles hébergent.

Le DSA inclut un code de bonnes pratiques contre la désinformation, qui a été renforcé en 2022. Trente-trois parties, dont les grands réseaux sociaux tels que Meta et TikTok et les géants du numérique tels qu'Adobe, Google et Microsoft, se sont engagées à démonétiser la diffusion de la désinformation, à garantir la transparence de la publicité politique, à améliorer les outils à disposition des utilisateurs pour signaler les fausses informations – ils sont massivement utilisés, comme le montre le baromètre du numérique de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), publié en début de semaine – et à fournir aux chercheurs un meilleur accès aux données pour accroître leur coopération. La recherche autour de la désinformation est cruciale. La collaboration des plateformes lui est nécessaire.

Le réseau social X s'est retiré en mai 2023 du code de bonnes pratiques contre la désinformation. Des enquêtes sont en cours. S'il s'avère que la réglementation n'a pas été respectée, des sanctions seront prises.

S'agissant de la guerre cognitive, Viginum joue depuis 2021 un rôle fondamental et reconnu – il est considéré, dans toutes les réunions à l'échelon européen, comme un service à la pointe de l'analyse technologique et de la compréhension des phénomènes de manipulation de l'information, permettant de détecter et de comprendre les menaces. La loi visant à sécuriser et à réguler l'espace numérique, dite loi SREN, défendue par mon prédécesseur et adoptée en mai 2024, permet de prendre les devants et dote l'Arcom de la possibilité

d'enjoindre aux opérateurs de respecter les interdictions de diffusion de contenus produits par les médias visés par des sanctions internationales.

En matière d'éducation aux médias et à l'information, nous avons fait en sorte que, au plus tard en 2027, tous les collégiens bénéficient chaque année d'une action d'éducation à la manipulation de l'information. La sensibilisation a déjà été mise en œuvre par de multiples canaux. Une circulaire de 2022 prévoit de généraliser l'éducation à la manipulation de l'information, de plus en plus cruciale à mesure que l'IA progresse. La formation de nos jeunes à la détection et à la compréhension de ces phénomènes est une composante essentielle de la lutte contre la manipulation de l'information.

S'agissant des Sala, l'IA est désormais omniprésente dans le domaine de la défense, tant dans l'espace cyber que sur le champ de bataille. Les conflits sont de plus en plus technologiques. Le règlement européen sur l'intelligence artificielle est le fruit d'une réflexion approfondie. Il distingue notamment les usages interdits, limités et à haut risque de la technologie, et leur fournit un cadre au sein duquel il appartient à chaque État membre de définir sa politique d'encadrement de la technologie.

Mme Valérie Bazin-Malgras (DR). À partir d'une simple description, l'IA générative peut fabriquer des images d'un réalisme inquiétant. De telles réalisations pourront servir à la désinformation, comme le font déjà les deepfakes, à la création d'une réalité alternative au service de motivations politiques préoccupantes dès lors qu'elles reposent sur le mensonge. Compte tenu du danger que représente l'utilisation malveillante de tels outils à l'égard de notre démocratie et de notre sécurité, il faut réagir. Que proposez-vous pour encadrer les images produites par l'IA générative en vue de prévenir de telles pratiques de désinformation et leurs conséquences dramatiques ?

Par ailleurs, les immenses capacités de l'IA lui permettent d'élaborer des clés de chiffrement complexes et des techniques de déchiffrement. Elle représente donc un enjeu majeur pour la sécurité des communications stratégiques. Elle peut être aussi bien un atout contre leur interception qu'une menace de déchiffrement de tout système de chiffrement. La France investit-elle dans des techniques de cryptographie à la hauteur de ces enjeux ?

Mme Clara Chappaz, ministre déléguée. L'usage d'images à des fins de manipulation de l'information a été constaté dans plusieurs pays européens, où mes homologues en ont subi les conséquences de plein fouet. Le règlement européen sur l'intelligence artificielle l'interdit. Nous veillerons à son respect. Sa transposition est en cours. Les autorités de contrôle seront nommées d'ici le mois d'août.

Certains disent que l'Europe régule tandis que d'autres innovent. Le travail mené à l'échelon européen en vue de réglementer les usages de l'IA me semble fondamental. Nous avons décidé, en Européens, et nous pouvons en être fiers, que nous ne voulons pas de certaines pratiques. Nous devons être fermes sur ce point. Par ailleurs, le règlement attache à tout contenu généré par l'IA, à des fins de manipulation ou non, des obligations de transparence, afin que quiconque y soit confronté soit pleinement conscient de ce dont il s'agit.

S'agissant du chiffrement, le développement de nouvelles technologies impose de monter en compétence. En novembre dernier, lors de la *European Cyber Week* à Rennes, j'ai annoncé la quatrième édition de l'appel à projets pour le développement de technologies

innovantes critiques. Nous avons reçu une quinzaine de dossiers. Nous devons nous assurer que nos opérateurs et nos entreprises de cybersécurité montent en compétence dans la compréhension de l'évolution des menaces et dans la façon d'y faire face, ce qui suppose de se maintenir à la pointe de la technologie, notamment en matière d'IA et d'informatique quantique.

Notre écosystème est vigoureux. Nous n'en avons pas moins l'intention de l'accompagner pour être à la hauteur des risques auxquels nous serons confrontés, parmi lesquels l'empoisonnement des données utilisées pour entraîner l'IA. Nos acteurs doivent se saisir des nouvelles technologies pour améliorer les protections et réduire les vulnérabilités.

Mme Catherine Hervieu (EcoS). L'objectif de la France est de devenir la première puissance militaire de l'IA en Europe et l'une des trois premières au monde. Les États-Unis investissent 500 milliards de dollars dans le programme Stargate. La LPM 2024-2030 prévoit de consacrer 2 milliards à ce domaine ; l'Amiad dispose d'une enveloppe de 300 millions par an. La France seule se heurte à des limites lorsqu'il s'agit d'investir dans les nouvelles technologies et de rattraper son retard. Le développement de l'IA serait plus performant à l'échelon européen.

Nous avons besoin de décisions politiques pour accélérer la transformation numérique à grande échelle. Les investissements actuels sont un début mais n'égalent pas ceux de nos compétiteurs extra-européens. Comment privilégier une logique à long terme au sein d'un cadre véritablement européen ?

Côté cyber, nos services publics et nos entreprises sont les cibles de menaces hybrides. L'intelligence économique est désormais prise au sérieux par nos entreprises et par l'État. Nous examinerons prochainement le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Les efforts entrepris doivent être poursuivis. La cybersécurité de l'État doit être renforcée afin de protéger nos données et les secteurs critiques. L'OS n° 4 de la RNS2022, intitulé *Une résilience cyber de premier rang*, est plus que jamais d'actualité à l'heure du rehaussement du niveau de cybersécurité des services publics. Quels investissements seront engagés pour consolider le socle numérique de l'État homogène et sécurisé ?

Le deuxième contrat stratégique de filière « Industries de sécurité » a été signé hier. Cette étape est encourageante ; quelles sont les suivantes ?

Mme Clara Chappaz, ministre déléguée. Le financement de la défense relevant du périmètre du ministère des armées, j'évoquerai plus généralement les moyens consacrés à l'IA, qui est une technologie éminemment duale.

Le Sommet pour l'action sur l'intelligence artificielle a été l'occasion d'annoncer des investissements à hauteur de 109 milliards, qui permettront de renforcer les infrastructures, et de renforcer notre ambition européenne. La présidente Ursula von der Leyen a indiqué que 200 milliards seront consacrés à l'IA, dont 50 milliards de fonds publics dans le cadre de l'initiative InvestAI pour financer des projets d'infrastructures et d'adoption de la technologie et 150 milliards d'investissement privé, afin de renforcer la collaboration entre ces deux sources de financement.

S’agissant de la cybersécurité à l’échelon européen, nous avons discuté, lors de la réunion ministérielle informelle des télécommunications du Conseil européen à Varsovie, de la priorité à donner à l’industrie de cybersécurité et de son articulation avec le plan ReArm Europe. Nous faisons en sorte de renforcer notre investissement dans l’écosystème cyber européen pour disposer de solutions permettant de répondre à la menace et nous assurer que nous ne dépendons pas entièrement de solutions extra-européennes.

Ces sujets seront abordés lors des négociations du cadre financier pluriannuel (CFP) européen, qui s’ouvriront prochainement à Bruxelles. L’IA, le cyber, le cloud et l’informatique quantique sont des technologies fondamentales pour nos infrastructures numériques seront au nombre de nos priorités.

La signature du deuxième contrat de filière « Industries de sécurité », dans le cadre du comité stratégique de filière (CSF), par les ministres Buffet et Ferracci et moi-même, est une étape importante. Cette deuxième feuille de route tire les enseignements de la précédente. Au début des années 2000, la cybersécurité ne représentait que 5 % de la filière, contre un tiers actuellement. Elle est donc au centre de sa stratégie et de son potentiel de développement.

Sa feuille de route inclut les thèmes majeurs et transversaux que sont l’accompagnement de l’écosystème privé, notamment grâce à la création d’un accélérateur accompagnant la montée en puissance des entreprises, le rapprochement entre le public et le privé, notamment grâce à la création d’une réserve cyber européenne au sein de laquelle les compétences de l’écosystème privé aideraient l’État à assurer sa cybersécurité, et la formation et l’attractivité des métiers de la cybersécurité, où environ 40 000 postes sont à pourvoir et où la proportion de travailleurs féminins est améliorable.

Mme Geneviève Darrieussecq (Dem). Même si la cybersécurité est un domaine technique, il faut, me semble-t-il, que chacun soit un talent. Les attaques cyber, particulièrement délétère pour les systèmes d’information des entreprises, notamment les petites, des administrations et des hôpitaux, au point de représenter des menaces lourdes, notamment sanitaires, réussissent parce que des gens laissent passer les virus informatiques.

Il nous faut donc une armée complète pour travailler dans le champ de la cybersécurité. La formation de toute personne qui touche à un ordinateur, à tous les niveaux des entreprises et des hôpitaux, est essentielle. Il en va de la cybersécurité comme de la santé : le soin va de pair avec la prévention. Comment bâtir un maillage, dans notre pays, d’espaces de cyberprotection et de cybersécurité pour former les acteurs et aider les entreprises à récupérer leurs données dans de bonnes conditions ? À quelle échelle ?

Par ailleurs, je soulève une question d’ordre général : qui veut déstabiliser l’Europe ? La Russie et la Chine, habituellement pointées du doigt, sont-elles les seules ? Les États-Unis n’ont-ils pas une posture agressive en matière de cybersécurité et d’usages dévoyés de l’IA ?

Mme Clara Chappaz, ministre déléguée. J’ai moi aussi, après plusieurs mois passés à m’intéresser de très près au numérique et à l’IA, le sentiment que tout un chacun doit y être formé. J’aurai besoin de vous dès l’examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité pour donner aux attaques cyber la place qu’elles méritent dans le débat public.

J’ai récemment lancé sur un réseau social professionnel un appel à témoignage visant à recueillir des récits d’attaques, convaincue que les meilleures protections sont la sensibilisation et la pédagogie. J’ai effectué un déplacement à l’hôpital de Bourg-en-Bresse, victime d’une attaque ayant détruit cinquante-deux serveurs. Les équipes, très bien préparées, ont réussi à s’en sortir mieux que d’autres ayant subi une attaque semblable. Ils avaient élaboré des processus, jusqu’à disposer de photos des câbles à débrancher en cas de cyberattaque.

Certes, la précision de leur anticipation a bénéficié du plan France Relance, ce qui prouve qu’il a des effets bénéfiques. Surtout, ils avaient aidé l’hôpital de Villefranche-sur-Saône, attaqué quelques mois plus tôt et lourdement affecté. C’est en échangeant avec leurs collègues qu’ils ont pris conscience de la menace et de la nécessité de l’anticiper. Le risque cyber a donc été ajouté à la liste des menaces exceptionnelles auxquelles les soignants doivent se préparer. Ils étaient donc prêts quand l’attaque, qui finit toujours par arriver, a eu lieu.

Forte de cette expérience, j’ai lancé un appel à témoignages, auquel j’ai reçu deux types de réponses : publiquement, des dizaines d’entreprises ont offert des solutions de protection ; en privé, les témoignages ont afflué. Nous étudions les moyens de les rendre publiques, car je suis persuadée que c’est en rendant publiques les cyberattaques que nous en développerons la prise de conscience et que nous en améliorerons l’anticipation.

D’ores et déjà, le Comcyber de la gendarmerie, dans le cadre de son service de proximité, se rend auprès des chefs d’entreprise, notamment de petites entreprises, pour leur faire prendre conscience de la réalité de la menace et de la nécessité de s’y préparer. Un patron de chocolaterie m’a indiqué qu’il n’aurait jamais imaginé être la cible d’une cyberattaque.

L’action des chambres de commerce et d’industrie (CCI) est exceptionnelle. J’ai constaté que les CCI du Nord et du Loiret proposent des sensibilisations et des formations. Le dispositif Conseillers numériques, lancé dans le cadre de la politique d’inclusion numérique et auquel je suis attaché, permet de diffuser des messages sur les risques cyber au plus près du terrain. Les Campus cyber et le réseau des Csirt (*computer security incident response team*) effectuent un travail de sensibilisation. La réserve citoyenne du numérique, créée par la loi de 2024 dite Sren (sécuriser et réguler l’espace numérique), est essentielle dans la mesure où nous devons associer les citoyennes et les citoyens aux questions numériques qui, si techniques qu’elles puissent paraître, concernent tout le monde.

Mme Anne Le Hénanff (HOR). L’actualisation de la Revue stratégique de cyberdéfense se fait attendre depuis de longs mois. Cette mise à jour aura-t-elle lieu ? Comment sera-t-elle intégrée dans la RNS, à laquelle elle est étroitement liée ? Quelle sera la place de l’IA ? En 2022, cette technologie était évoquée ; il n’est plus possible de se contenter d’un paragraphe de trois lignes. Quelles seront vos préconisations ?

Je suis convaincue de la nécessité d’associer la population aux enjeux de défense, comme le font les pays du nord de l’Europe, afin d’assurer la résilience pleine et entière de la nation. Il ne s’agit pas que d’une affaire de militaires. Quelle est votre position à ce sujet ? Parvenez-vous à convaincre les militaires que la cyberrésilience doit inclure les citoyens ?

Mme Clara Chappaz, ministre déléguée. L'actualisation de la Revue stratégique de cyberdéfense est en cours. Je ne peux en dire plus, sinon que je serai attentive à toute suggestion émanant de cette commission et à la bonne coordination de nos travaux. Le Président de la République aura sans doute l'occasion d'en parler prochainement.

Le cyber n'est pas un sujet d'expert. Nous devons nous appuyer sur le tissu associatif et sur les citoyens eux-mêmes, dans le cadre de la réserve citoyenne du numérique. Nous travaillons à son lancement, en veillant à y intégrer une dimension cyber.

M. le président Jean-Michel Jacques. Nous en venons à l'intervention d'un orateur individuel.

Mme Stéphanie Galzy (RN). Les récents conflits, notamment en Ukraine, ont démontré le rôle central des drones, qu'ils soient de reconnaissance, armés ou suicides. Ces technologies, combinées aux avancées de l'IA, redéfinissent les stratégies militaires et imposent une adaptation rapide. Comme l'aviation lors de la Première guerre mondiale, les drones autonomes bouleversent la manière de conduire la guerre et sont appelés à jouer un rôle majeur dans les futurs théâtres d'opérations.

Tandis que la France et l'Europe annoncent leur réarmement, notre pays accuse un retard en matière de drones autonomes et d'IA appliquée à la défense, qui sont des enjeux stratégiques en matière militaire et de souveraineté. Quelle place ces technologies occupent-elles dans la modernisation de nos armées ? Quels moyens sont déployés pour garantir une réelle souveraineté technologique et éviter une dépendance à des technologies étrangères ?

Mme Clara Chappaz, ministre déléguée. Mes collègues Éric Lombard et Sébastien Lecornu ont récemment annoncé le plan de financement de l'économie de défense. L'innovation technologique y aura toute sa place. Au cours des dernières années, notre écosystème de défense n'a pas toujours trouvé les financements nécessaires pour se développer. Désormais, l'écosystème d'innovation est au cœur du projet. BPIFrance a pris des dispositions en ce sens. Nous ferons en sorte que nos entreprises innovantes en bénéficient.

M. le président Jean-Michel Jacques. Madame la ministre, au nom de la commission, je vous remercie de vos réponses.

*

* *

La séance est levée à dix-huit heures cinq.

*

* *

Membres présents ou excusés

Présents. – Mme Valérie Bazin-Malgras, Mme Geneviève Darrieussecq, Mme Stéphanie Galzy, M. Frank Giletti, Mme Catherine Hervieu, Mme Emmanuelle Hoffman, M. Jean-Michel Jacques, M. Pascal Jenft, Mme Anne Le Hénanff, Mme Josy Poueyto, Mme Marie Récalde, M. Aurélien Saintoul, Mme Sabine Thillaye

Excusés. – M. Christophe Bex, Mme Anne-Laure Blin, M. Frédéric Boccaletti, M. Manuel Bompard, M. Elie Califer, M. Bernard Chaix, Mme Cyrielle Chatelain, M. Paul Christophe, M. Damien Girard, Mme Lise Magnier, M. Jean-Philippe Nilor, Mme Natalia Pouzyreff, Mme Mereana Reid Arbelot, M. Arnaud Saint-Martin, M. Mikaele Seo, M. Thierry Tesson, M. Boris Vallaud, M. Stéphane Viry, M. Éric Woerth