ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

# Compte rendu

## Commission de la défense nationale et des forces armées

— Examen, ouvert à la presse, des conclusions de la mission flash sur les défis de la cyberdéfense (co-rapporteurs : Mme Anne Le Hénanff et M. Frédéric Mathieu).

Mercredi
17 janvier 2024
Séance de 9 heures 30

Compte rendu n° 34

SESSION ORDINAIRE DE **2023-2024**

**Présidence de M. Jean-Pierre Cubertafon,** *Vice-président*

ASSEMBLÉE NATIONALE

*La séance est ouverte à neuf heures trente.*

**M. le président Jean-Pierre Cubertafon.** Madame la rapporteure, Monsieur le rapporteur, mes chers collègues, nous sommes réunis ce matin pour entendre les conclusions des rapporteurs de la mission flash sur les défis de la cyberdéfense.

Avant toute chose, je tiens à excuser M. le Président Thomas Gassilloud pour son absence. Il est en effet actuellement en déplacement en Afrique avec nos collègues Benoît Bordat, François Piquemal et Anna Pic.

La commission de la Défense nationale et des forces armées a créé une mission flash sur les défis de la cyberdéfense le 15 mars 2023. Elle en a désigné rapporteurs Mme Anne Le Hénanff et M. Frédéric Mathieu, ici présents.

Dans le cadre de leur mission flash, les rapporteurs ont conduit 25 auditions, à l'occasion desquelles ils ont auditionné des représentants du ministère des Armées mais également de l'ANSSI, du SGDSN, du ministère de l'Intérieur, du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur et de la Recherche. Ils ont également pu s'entretenir avec des journalistes, des représentants d'ONG ainsi que des représentants d'entreprises de la BITD.

Par ailleurs, les rapporteurs ont effectué trois déplacements sur le territoire national et un déplacement à l'étranger. Sur le territoire national, ils se sont rendus à la DGA-MI, à Bruz, au groupement de la cyberdéfense des armées, à Saint-Jacques-de-la-Lande, à la 807e compagnie de transmissions de l'armée de Terre, à Saint-Jacques-de-la-Lande également, au commandement des systèmes d'information et de la communication de l'armée de Terre, à Cesson-Sévigné, ainsi qu'au Centre Support Cyberdéfense de la Marine nationale, à Brest. Ils se sont également rendus en Finlande et en Estonie.

Je souhaite d'emblée féliciter nos deux rapporteurs pour la très grande qualité de leur travail et pour leur investissement. Il s'agit d'un sujet majeur pour nos armées, consacré d'ailleurs comme tel dans la LPM, le cyberespace étant en effet un des nouveaux champs de conflictualité avec l'espace et les fonds marins. Nous avons hâte d'entendre vos conclusions qui, au regard de votre programme de travail, promettent d'être particulièrement riches et denses. Sans plus attendre, je vous cède la parole.

**Mme Anne Le Hénanff, rapporteure.** Merci Monsieur le Président, mes chers collègues, je suis très heureuse de vous présenter les conclusions de notre mission flash sur les défis de la cyberdéfense. Mon collègue et moi souhaitons d'emblée remercier le président Thomas Gassilloud de nous avoir confié cette mission flash, sur un sujet dont nous estimons qu'il est à la fois capital et encore trop peu estimé à sa juste valeur. Je souhaite également remercier mon collègue co-rapporteur Frédéric Mathieu, avec lequel j'ai pris plaisir à travailler. Nos relations de travail ont été excellentes tout le long de la mission, et j'espère qu'il en dira autant !

Avant de rentrer dans le vif du sujet, nous souhaitions d'emblée faire quelques remarques d'ordre méthodologique.

Dans le cadre de notre mission flash, nous nous sommes intéressés aux défis de la « cyberdéfense ». Cette notion a été entendue au sens des trois doctrines de lutte informatique du ministère des Armées que sont la lutte informatique défensive, dite LID, la lutte informatique offensive, la LIO et la lutte informatique d'influence, L2I.

Nous avons également inclus dans le périmètre de notre mission flash la cybersécurité, la cyberprotection et, surtout, la cyber-résilience ; notion qui nous est particulièrement chère.

En tant que membres de la commission de la Défense, nous avons bien entendu orienté nos travaux avec un prisme « défense », toutefois, convaincus que nous sommes de la nécessité d'appréhender cette question au-delà du seul périmètre du ministère des Armées, nous avons également fait le choix de nous intéresser à cette question à l'échelle interministérielle, et en l'occurrence, à l'échelle du SGDSN, autorité de tutelle de l'ANSSI.

Comme l'a indiqué le président, nous avons conduit 25 auditions, à l'occasion desquelles nous nous sommes entretenus avec des représentants des états-majors, directions et services du ministère des Armées bien sûr, mais également avec des représentants de l'ANSSI, du SGDSN et du ministère de l'Intérieur. En vertu de cette approche globale, nous avons choisi d'élargir notre prisme d'analyse en auditionnant des représentants du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur et de la Recherche. Nous nous sommes également entretenus avec des journalistes, avec des représentants d'ONG, et, bien sûr, des représentants d'entreprises de la BITD.

En complément des auditions conduites à l'Assemblée nationale, nous avons effectué trois déplacements sur le territoire national et un déplacement à l'étranger. Nous étions en effet convaincus qu'il était absolument indispensable de nous rendre sur le terrain pour appréhender la cyberdéfense de manière concrète, opérationnelle, au plus près des acteurs concernés. Sur le territoire national, nous nous sommes rendus à la DGA-MI, à Bruz, au groupement de la cyberdéfense des armées du COMCYBER et à la 807$^{e}$ compagnie de transmissions de l'armée de Terre, à Saint-Jacques-de-la-Lande, au commandement des systèmes d'information et de la communication de l'armée de Terre, à Cesson-Sévigné, ainsi qu'au Centre Support Cyberdéfense de la Marine nationale, à Brest.

Nous avons également souhaité nous rendre à l'étranger pour nous enquérir de la manière dont la cyberdéfense est appréhendée par d'autres États. Nous nous sommes ainsi rendus en Finlande et en Estonie, deux États particulièrement avancés dans les domaines de la cyber-résilience et de la cyberdéfense, qui peut s'expliquer par leur situation géographique et le contexte géopolitique, je pense notamment à la guerre en Ukraine.

Fruit de ces travaux qui, comme vous pouvez vous en douter, ont été particulièrement denses, nous formulons 35 recommandations, regroupées en 6 défis que nous nous attellerons à vous présenter dans le cadre de ce propos introductif. Ces recommandations sont évidemment le résultat des échanges nourris que nous avons pu avoir avec l'ensemble de nos interlocuteurs mais ils ont également le fruit de nos propres expériences. En ce qui me concerne, de par mon expérience d'élue locale à Vannes en charge du numérique depuis de nombreuses années, j'ai toujours gardé à l'esprit l'importance de ce sujet pour nos territoires.

Nous tenons à remercier l'ensemble des personnes que nous avons rencontrées lors de nos travaux. Les échanges que nous avons eus, les réflexions qu'ils ont partagées, leur investissement pour nous accueillir lors de nos déplacements et leur disponibilité nous ont

permis de vous présenter aujourd'hui nos conclusions. Merci à eux pour le temps qu'ils nous ont consacrés.

**M. Frédéric Mathieu, rapporteur.** Je souhaite, en préambule, remercier également ma collègue Anne Le Hénanff pour la qualité de notre coopération et le travail fourni. Ce fut un vrai plaisir de travailler à vos côtés, chère collègue. Je m'associe pleinement aux remerciements formulés vis-à-vis des personnes avec lesquelles nous avons travaillé.

Avant de vous présenter les défis de la cyberdéfense que nous avons identifiés et les recommandations associées, permettez-nous de vous présenter brièvement l'écosystème de cyberdéfense ; prérequis indispensable à la bonne compréhension de nos conclusions.

Le cyberespace se structure en trois couches indissociables, d'où procèdent toutes les menaces :

1/ une couche physique, constituée des équipements, des systèmes informatiques et de leurs réseaux ayant une existence matérielle (et donc une territorialité qui ouvre sur un droit national, voire international) ;

2/ une couche logique, constituée de l'ensemble des données numériques, des logiciels, des processus et outils de traitement, de gestion et d'administration de ces données, ainsi que de leurs flux d'échanges, implantés dans les matériels pour leur permettre de rendre les services attendus ;

3/ et une couche cognitive, également appelée couche informationnelle, constituée des informations et des interactions sociales de toutes sortes qui se trouvent dans le cyberespace et des personnes qui peuvent déclarer plusieurs identités numériques.

Au-delà de la notion de « défendabilité » des systèmes, la cyberdéfense au sein du ministère des Armées est déclinée en cohérence avec les six missions définies par la revue stratégique de cyberdéfense publiée en février 2018 :

1/ prévenir : il s'agit de faire prendre conscience aux utilisateurs du risque représenté par la numérisation des organisations ou des équipements qu'ils servent ;

2/ anticiper : il s'agit d'évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte. Cette mission incombe à l'Agence nationale de sécurité des systèmes d'information (ANSSI), en coordination avec les services de renseignement et le Commandement de la cyberdéfense (COMCYBER) sur le périmètre du ministère des Armées ;

3/ protéger : il s'agit de diminuer la vulnérabilité de nos systèmes informatiques, à la fois en compliquant la tâche des attaquants potentiels et en facilitant la détection des cyberattaques ;

4/ détecter : il s'agit de rechercher des indices d'une éventuelle cyberattaque en cours. Cette mission relève de la responsabilité du COMCYBER et des unités subordonnées au ministre des Armées. Pour compléter ses informations, il sollicite ses partenaires nationaux et internationaux ;

5/ réagir : il s'agit de résister à une cyberattaque afin qu'elle n'empêche pas la poursuite de notre activité. Dans la plupart des cas, le COMCYBER déclenche alors une opération de lutte informatique défensive, en liaison avec l'ANSSI. Elle peut entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense, voire du ministère des Armées (par exemple, la saisie de la justice, une action diplomatique ou une mesure de rétorsion économique) ;

6/ attribuer : il s'agit de préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution ; la décision d'attribution appartenant, *in fine*, aux plus hauts responsables politiques.

Ainsi, les actions de prévention et de protection concernent les systèmes informatiques du ministère des Armées, tandis que les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs.

**Mme Anne Le Hénanff, rapporteure.** Par ailleurs, les opérations dans le cyberespace reposent sur trois doctrines : la lutte informatique défensive (LID), qui regroupe l'ensemble des actions, techniques ou non, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle ; la lutte informatique offensive (LIO), qui regroupe l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels, pour produire des effets à l'encontre d'un système adverse afin d'en altérer la disponibilité ou la confidentialité des données et la lutte informatique d'influence (L2I), qui désigne les opérations militaires conduites de façon autonome ou en combinaison avec d'autres opérations dans la couche informationnelle du cyberespace afin de détecter, caractériser et contrer les attaques, appuyer la communication stratégique, renseigner ou faire de la déception.

Le cyberespace constitue donc désormais un espace de manœuvre et de confrontation à part entière, au même titre que les milieux terrestres, maritime, aérien, et extra-atmosphérique. Le cyberespace est un milieu transverse dont les activités sont nécessairement en interaction avec les milieux conventionnels : terre, mer, air, espace, notamment en matière de champs électromagnétique et informationnel.

L'action dans ou depuis le cyberespace peut ainsi produire des effets dans l'ensemble des milieux et des champs. Par exemple, une attaque cyber peut faire dévier de sa route un satellite. Réciproquement, une action dans ces milieux et champs peut produire des effets dans le cyberespace, comme la destruction physique d'un serveur.

Dans ce contexte, le cyberespace a acquis une valeur stratégique permettant de garantir la liberté d'action des forces dans les autres milieux et champs. Or, la menace est multiforme, permanente, non territorialisée et peut avoir des conséquences à tous les niveaux tactiques, à l'avant comme à l'arrière. Ce milieu doit par conséquent être pris en compte dans la manœuvre pour se protéger et pour saisir les opportunités d'agir. Surtout, il doit être pris en compte dès la phase de compétition du *continuum* « compétition-contestation-affrontement », au quartier comme en mission.

En outre, il existe des spécificités de milieu évidentes dans l'exploitation du volet cyber par les trois armées. Un sous-marin n'est pas soumis à la même menace cyber qu'un PC de division installé en zone industrielle d'une ville ou qu'un avion militaire posé sur une base

aérienne de théâtre. De même, l'environnement numérique adverse d'une force navale, terrestre ou aérienne est intimement lié à son milieu.

Les trois volets de la politique de cyberdéfense du ministère des Armées (LID, LIO et L2I) permettent aux trois armées de prendre en compte ces dimensions (se protéger, se défendre et agir) de manière adaptée et complémentaire grâce à une organisation assurant la cohérence d'ensemble du modèle cyber du ministère tout en respectant les spécificités des armées.

Mais si les doctrines sont une référence, elles ne constituent pas un carcan. Elles définissent les principes et les responsabilités et doivent s'adapter à l'emploi. Dans un domaine aussi jeune que les opérations dans le cyberespace, il est pertinent qu'elles soient revues régulièrement avec l'ensemble de la communauté cyber mais aussi plus largement la communauté militaire des opérations car tout évolue très rapidement. L'apparition dans le champ doctrinal du concept des opérations multi milieux multi champs dans le concept d'emploi des forces de 2021 traduit d'ailleurs bien cet état de fait.

**M. Frédéric Mathieu, rapporteur.** Le schéma qui s'affiche derrière nous vous présente une version simplifiée de l'écosystème de la cyberdéfense à l'échelle de l'État.

S'agissant des acteurs de la cyberdéfense au sein du ministère des Armées, l'acteur central est le commandement de la cyberdéfense (COMCYBER). Placé sous l'autorité directe du CEMA, le COMCYBER est un commandement opérationnel qui rassemble l'ensemble des forces de cyberdéfense sous une autorité interarmées déployé sur plusieurs emprises à Paris et à Rennes. Le COMCYBER effectue ses missions par délégation de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est responsable de la cyberdéfense et de la cybersécurité des administrations publiques, des entreprises et, singulièrement, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE).

Créé en mai 2017, le COMCYBER est en charge de la conception, de la planification et de la conduite des opérations de cyberdéfense, ainsi que de la défense des systèmes d'information des armées, directions et services du ministère des Armées (à l'exception de ceux de la DGSE et de la DRSD) ; de la stratégie de cyberdéfense par la coordination des contributions des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense et par la mise en cohérence du modèle de cyberdéfense du ministère des Armées ; de la dimension capacitaire de la politique de cyberdéfense par l'élaboration de la politique des ressources humaines de cyberdéfense, par la coordination de la définition des besoins techniques spécifiques à la cyberdéfense et par la gestion de la réserve de cyberdéfense.

Autre acteur de la cyberdéfense au sein du ministère des Armées, la DGA constitue l'expert technique référent du ministère des Armées.

De manière générale, la DGA est responsable de la conception et de la réalisation des systèmes permettant de garantir aux forces, dans la durée, la résilience cyber des capacités qu'elles opèrent, et d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace.

Cette mission se décline selon quatre axes :

1/ porter à un niveau adapté au niveau de la menace la cybersécurité des systèmes numériques et des systèmes d'armes afin d'être résilient face aux agressions cyber ;

2/ équiper nos forces armées de systèmes leur permettant d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace, c'est-à-dire de conduire des actions dans les trois domaines de lutte informatique ;

3/ orienter, maintenir et développer les capacités technologiques et industrielles nécessaires, en cohérence avec la stratégie nationale de cyberdéfense ;

4/ accroître la cybersécurité de la BITD et contribuer à la cyberdéfense de la Nation.

Enfin, le troisième acteur principal du ministère des Armées dans le domaine de la cyberdéfense est la DGSE. Elle participe à la protection des intérêts fondamentaux de la France par des actions de renseignement ainsi qu'à la compréhension et à la réduction de la menace cyber (criminelle ou d'État).

Au titre de cette mission, la DGSE est membre du centre de coordination des crises cyber (C4), qui regroupe l'ANSSI, la DGA, le COMCYBER et la DGSI, et partage ses renseignements au sein de cette comitologie interministérielle. Sur le territoire national, sur autorisation du Premier ministre après avis de la CNCTR, la DGSE met en œuvre toutes les techniques de recueil du renseignement autorisées par le code de la sécurité intérieure, selon le principe de proportionnalité. À l'étranger, la DGSE utilise tous types de techniques de recueil du renseignement dont elle dispose.

Par anticipation sur une action hostile pouvant toucher la France, le renseignement sur la menace cyber cherche à informer sur les acteurs, étatiques ou criminels, connus pour nourrir des projets agressifs dans l'espace numérique ainsi que sur les outils et les services commercialisés pour mettre en œuvre ces projets. En complément, par réaction à une action hostile ayant touché la France, le renseignement sur la menace aura pour mission d'identifier l'auteur de l'action et son donneur d'ordre.

**Mme Anne Le Hénanff, rapporteure.** D'autres acteurs au sein du ministère des Armées jouent un rôle prépondérant en matière de cyberdéfense : la DIRISI, la DRSD, la DPID ou encore la DGNUM sont autant d'entités qui participent, directement ou indirectement, aux capacités de cyberdéfense du ministère. Les trois armées sont évidemment également parties prenantes de la cyberdéfense du ministère des Armées, selon des modalités en cours d'évolution, mais nous y reviendrons.

Au-delà du ministère des Armées, l'ANSSI est l'acteur principal de la cyberdéfense au sein de l'État. Créée en 2009 et rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), la principale mission de l'ANSSI est d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des administrations, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE), auprès desquels elle exerce par ailleurs une mission de conseil et de soutien.

De son côté, la DGSI, membre du premier cercle des services de renseignement, est la seule entité qui peut exercer sa mission de cyberdéfense sur le territoire national aussi bien dans un cadre judiciaire que de renseignement. Lorsqu'une cyberattaque menace les intérêts fondamentaux de la Nation, la DGSI, agissant au titre de ses missions de contre-ingérence, de

contre-espionnage et de contre-terrorisme, peut mettre en œuvre des techniques de recueil du renseignement dans le cadre de ses investigations.

Plus spécifiquement, la DGSI suit les modes opératoires de nos attaquants cyber susceptibles de porter atteinte aux intérêts fondamentaux de la Nation et agit, de manière proactive ou réactive, pour contrer ces menaces.

Après cette présentation des concepts, de la doctrine et des acteurs de la cyberdéfense, venons-en aux défis que nous avons identifiés et que le ministère des Armées, et plus largement, l'ensemble des services de l'État, devra relever pour doter la France d'une puissance cyber de tout premier rang. Ces défis sont au nombre de six : premièrement, le défi de la gouvernance ; deuxièmement, le défi des ressources humaines ; troisième défi : le défi juridique ; quatrième défi : le capacitaire ; le cinquième défi concerne la prospective et enfin le défi de la transparence.

Le premier défi est le défi de la gouvernance. À l'issue de nos travaux, nous avons acquis la conviction que la politique de cyberdéfense de l'État gagnerait à être plus lisible et devrait être appréhendée de manière globale pour renforcer la cyber-résilience de la Nation. Nous avons en effet la conviction que la culture de la cybersécurité ne peut pas se décréter depuis un sommet… et diffuser au sein de la société sans cette approche globale. Cela impliquera notamment de renforcer les relations entre l'ANSSI et les armées, en cas de crise cyber majeure dans le secteur civil. Ce rapprochement est en cours, avec la perspective des Jeux olympiques et paralympiques de 2024, mais il devra encore être renforcé pour faire face aux défis de demain. Au demeurant, au-delà de la seule ANSSI, c'est bien l'ensemble des entités du secteur civil (collectivités territoriales et leurs établissements publics, établissements de santé, mais également opérateurs d'importance vitale et opérateurs de services essentiels) qui devraient pouvoir bénéficier des savoir-faire des armées en cas de crise cyber majeure.

Ce rapprochement est d'autant plus pertinent de notre point de vue que les effectifs de l'ANSSI sont limités, et singulièrement ceux de son centre de veille et d'alerte, et que la charge de travail qui pèsera sur elle ne fera qu'augmenter avec la directive NIS 2. Le recours par l'ANSSI à des prestataires privés de réponse aux incidents de sécurité est d'ailleurs la preuve qu'elle ne peut répondre seule à l'ensemble des cyberattaques qui frappent notre pays, cyberattaques qui ne vont cesser de se multiplier. Nous sommes d'ailleurs favorables à une augmentation des effectifs de ce centre d'alerte et de veille de l'ANSSI.

**M. Frédéric Mathieu, rapporteur.** De leur côté, les armées sont en train d'acquérir des compétences nouvelles en matière de cyberdéfense grâce à la mise en place de la communauté cyber des armées. Annoncée en filigrane lors des débats sur la LPM, la création d'une « communauté cyber des armées » a été officialisée en novembre 2023. En effet, au-delà des moyens financiers et humains, le COMCYBER indiquait en avril 2023 devant notre commission qu'un effort particulier serait fait pour adapter les modalités et les niveaux d'action de la cyberdéfense. Si certaines actions peuvent être conduites de loin dans le cyberespace, d'autres nécessitent d'être à proximité des cibles. Cette diffusion de la cyberdéfense au sein des trois armées, au plus près des bases et des régiments, contribuera sans doute au renforcement de la cyber-résilience du ministère et, plus globalement, de la Nation.

S’agissant plus spécifiquement des collectivités territoriales, de leurs établissements publics et des établissements de santé, nous estimons qu’il est temps de franchir un nouveau cap en matière de cybersécurité. Les trop nombreux exemples de cyberattaques ayant frappé des collectivités territoriales et des établissements de santé prouvent qu’il est désormais urgent de rehausser le niveau d’ambition en la matière. Concrètement, nous estimons qu’il faut instaurer l’obligation de diligenter, à intervalles réguliers, des « contrôles techniques » en cybersécurité, notamment en lien avec le ministère de l’Intérieur et le commandement du ministère de l’Intérieur dans le cyberespace – nouveau nom du commandement de la Gendarmerie dans le cyberespace – sous la responsabilité des préfets des zones de défense et des préfets de région. Nous avons pu apprécier concrètement les compétences et les savoir-faire des gendarmes en matière de cyberdéfense. Nous savons ce qu’ils peuvent apporter à ces entités et, ce faisant, contribuer à la cyber-résilience de la Nation.

**Mme Anne Le Hénanff, rapporteure.** Mais la cyber-résilience de la Nation impliquera également de renforcer l’éducation à la cybersécurité à l’école en vue de diffuser une culture de l’hygiène numérique au sein de la population. De ce point de vue, l’école a un rôle primordial à jouer. En formant les jeunes au risque cyber dès l’école, un très grand nombre de cyberattaques pourraient être évitées. Il n’est en effet plus à démontrer que la sensibilisation accompagnée de l’adoption de réflexes simples avant, pendant et après une attaque de nature cyber permet d’en limiter les impacts, voire d’éviter celle-ci. Le ministère de l’Éducation nationale devra donc prendre toute sa part à cet effort global de la Nation.

En outre, renforcer la cyber-résilience de la Nation impliquera de féminiser les recrutements des agents numériques et cyber de l’État afin d’élargir le vivier de compétences et de talents ouvert au recrutement. Cela vaut évidemment pour les services de l’État mais également dès l’école secondaire, en luttant efficacement contre les stéréotypes de genre et en incitant les jeunes filles à s’engager dans cette voie professionnelle.

**M. Frédéric Mathieu, rapporteur.** Par ailleurs, afin d’améliorer le niveau de cyber-résilience de la Nation, la participation à des exercices est indispensable. Dans le cadre de nos travaux, nous avons été alertés sur la faible participation des armées et des services de l’État aux exercices cyber organisés à l’échelle internationale. Nous n’avons par ailleurs pas eu connaissance d’exercices cyber organisés par la France et en France à destination de nos partenaires. Nous estimons pourtant cela indispensable. D’ailleurs, s’agissant de la nature de ces exercices, nous avons acquis la conviction qu’il était nécessaire d’organiser des exercices en conditions réelles, à la fois à l’échelle interministérielle mais également avec des États alliés dans le cadre de coopérations bilatérales. Nous pensons d’ailleurs que cela permettait de renforcer utilement le lien armées – Nation et que les populations seraient d’autant plus sensibilisées face au risque cyber si les conséquences d’une cyberattaque – par exemple l’arrêt d’une centrale électrique pendant quelques heures – sont ressenties *in concreto* par les populations dans le cadre de ces exercices.

Enfin, lorsque nous appelons de nos vœux un renforcement de la cyber-résilience de la Nation, nous pensons évidemment à l’ensemble du territoire national, et y compris, donc, les territoires ultra-marins. De ce point de vue, nous pensons qu’il est impératif d’élaborer une stratégie spécifique pour renforcer la cybersécurité dans les DROM-COM, qui sont particulièrement vulnérables face au risque de cyberattaques.

**Mme Anne Le Hénanff, rapporteure.** Venons-en désormais au deuxième défi : le défi des ressources humaines. Les difficultés de recrutement et de fidélisation du ministère des Armées dans le domaine de la cyberdéfense sont connues. Toutefois, le ministère des Armées possède de nombreux atouts pour attirer les talents et plusieurs pistes permettraient de mieux recruter, former et fidéliser les agents cyber du ministère.

Tout d'abord, même si cela peut paraître évident, il convient de rappeler que le ministère des Armées est en concurrence avec les secteurs publics et privés dans le cadre du recrutement des talents cyber. De ce fait, les difficultés de recrutement du ministère ne lui sont pas exclusivement imputables. Il est notamment tributaire du manque d'offre de formations dans les établissements d'enseignement supérieur, même si on note ces dernières années un développement accru de ces offres et une ouverture à un panel plus large d'étudiants. J'en veux pour preuve la création par le COMCYBER d'un parcours universitaire entre l'École Polytechnique et l'EPITA dédié à la cyberdéfense. Toutefois, au-delà des seules grandes écoles, il est absolument indispensable que l'offre de formation en matière de cybersécurité et de cyberdéfense soit étendue. Cette mission incombera en premier lieu au ministère de l'Enseignement supérieur et de la Recherche.

Par ailleurs, les études démontrent que le recours à l'apprentissage est un moyen très efficace pour recruter et fidéliser les agents cyber. Le ministère des Armées est pleinement engagé dans cette voie avec la création d'un BTS à Saint-Cyr l'École et au lycée Naval à Brest. Cette politique doit être renforcée.

Une seconde piste pour améliorer le recrutement et la fidélisation est celle relative au développement des parcours croisés au sein des services de l'État. Si le critère de la rémunération est souvent mis en avant pour justifier les difficultés de recrutement et de fidélisation, l'absence de visibilité sur la carrière joue également. Aujourd'hui, ces parcours croisés restent encore trop peu développés et la concurrence entre les services reste de mise. Ces derniers peuvent également s'effectuer sous la forme d'aller et retour entre les armées et le secteur privé, dans le respect des règles déontologiques qui encadrent ces départs et de l'article 42 de la loi de programmation militaire qui a mis en place un mécanisme pour lutter contre les ingérences étrangères dans le cadre de recrutements.

**M. Frédéric Mathieu, rapporteur.** En outre, la feuille de route relative à la féminisation des agents cyber de l'État que nous appelons de nos vœux gagnerait à être déclinée au sein du ministère des Armées. Celui-ci prend d'ores et déjà des initiatives dans le cadre du plan relatif à l'égalité professionnelle entre les femmes et les hommes, qui doivent être poursuivies.

Les agents cyber comprennent également les réservistes de cyberdéfense, qui peuvent jouer un rôle fondamental à la fois pour le ministère des Armées mais aussi pour la cyber-résilience de la Nation dont ils pourraient être de véritables ambassadeurs. Dans le plan réserve 2035, la trajectoire est fixée à 500 réservistes de cyberdéfense. Le ministère des Armées indique qu'elle sera consolidée en fonction des besoins et, si elle est soutenue, par la création de postes permanents dédiés à l'animation ou à la formation. Cette trajectoire nous semble insuffisante pour irriguer l'ensemble des armées. Nous estimons donc qu'il est indispensable de recruter davantage de réservistes cyber.

Venons-en désormais au troisième défi : le défi juridique. Même si cela est peu connu, la cyberdéfense comprend une dimension juridique relativement forte, en particulier s'agissant du cadre juridique des opérations militaires dans le cyberespace. Nous avons identifié quatre enjeux dans ce domaine.

Le premier enjeu a trait à la prise en compte des spécificités des armées dans le cyberespace dans le processus d'élaboration des normes. Il s'agit là d'un impératif absolu, notamment à l'échelle européenne, qui doit être pleinement pris en considération.

Le deuxième enjeu a trait au recours par les agents du ministère des Armées aux réseaux sociaux. Nous ne nous étendrons pas sur les exemples précis qui ont été portés à notre attention dans le cadre de nos travaux à cet égard. Toutefois, nous sommes en mesure de vous indiquer qu'il s'agit d'un véritable enjeu, et singulièrement parmi les plus jeunes recrues. Sans rentrer dans les détails, nous déplorons qu'une utilisation trop légère des réseaux sociaux ait pu parfois aboutir, involontairement, à une divulgation d'informations protégées par le secret de la défense nationale. Un guide du bon usage des réseaux sociaux a été adopté en 2021 pour les agents du ministère des Armées. Il rappelle le principe de discrétion professionnelle des agents du ministère, militaires comme civils. Une interdiction pure et simple ne serait ni possible, ni souhaitable. En revanche, la conduite d'une réflexion sur les voies juridiques envisageables pour mieux encadrer le recours aux réseaux sociaux, singulièrement en OPEX ou lors des exercices de préparation opérationnelle, nous apparaît souhaitable.

Le troisième enjeu a trait à notre politique d'exportation des biens à double usage dans le domaine cyber, et singulièrement des armes cyber offensives et des logiciels à base d'intelligence artificielle dans le domaine informationnel. Deux affaires ont défrayé la chronique ces dernières années, s'agissant des logiciels de cyber-espionnage : l'affaire Pegasus et l'affaire Predator. Sans rentrer dans les détails, ces deux affaires montrent qu'il est indispensable de réfléchir à une meilleure régulation des armes cyber offensives et de leurs exportations. S'agissant de la cyberdéfense, la DGA a indiqué que la France n'exporte pas d'autres systèmes que les produits sur étagère proposés par des sociétés duales, dans le cadre du régime de contrôle de l'exportation de biens à double usage d'une part, et les systèmes de cyberprotection et de lutte informatique défensive en tant que constituants d'un système d'armes (aériens ou navals par exemple), dont l'export relève du régime de contrôle des matériels de guerre, d'autre part. Elle a également indiqué que la France n'exporte aucun système ou sous-système cyber offensif.

Enfin, nous estimons nécessaire de procéder à une évaluation juridique afin de déterminer notre capacité à répondre par notre corpus juridique national et international actuel au mercenariat dans le domaine de la cyberdéfense. Nous ne sommes pas convaincus que le droit, et singulièrement le droit international, réponde à l'émergence de cette nouvelle catégorie d'acteurs. Nous ne sommes toutefois pas en mesure d'arrêter clairement notre position, et reconnaissons que le débat est ouvert. La clarification de cette situation nous semble indispensable, eu égard à la multiplication de ces acteurs et à leur potentielle nuisance.

**Mme Anne Le Hénanff, rapporteure.** Le quatrième défi est le défi capacitaire. Un premier ensemble d'enjeux a trait à notre souveraineté numérique.

Vous n'êtes pas sans ignorer les risques que fait peser le recours à des logiciels étrangers dans nos systèmes d'information et nos systèmes d'armes, et singulièrement eu

égard aux règles d'extraterritorialité du droit américain – mais pas que – ou encore des dispositions législatives adoptées par des États comme les États-Unis ou la Chine pour collecter, en toute légalité, nos données. À ce jour, le ministère des Armées n'exclut pas le recours à des solutions étrangères, y compris sur étagère, et ce tant pour ses systèmes d'armes que pour ses systèmes d'information, dès lors qu'elle estime que le risque est maîtrisé. En ce qui nous concerne, nous pensons qu'il est absolument indispensable de limiter au strict nécessaire le recours aux solutions étrangères dans nos systèmes d'armes. La présence de portes dérobées dans des solutions étrangères permettant à l'État fournisseur d'espionner l'État client n'est un secret pour personne. Les mesures prises pour réduire les risques sont salutaires. Mais cela suppose d'être en mesure de détecter les éventuelles portes dérobées installées sur les solutions étrangères. Or, comme nous avons pu l'entendre en audition, si on estime qu'il n'y a pas de cyberattaque, cela peut vouloir dire deux choses : soit il n'y en a effectivement pas, et tout va bien ! soit il y en a une que nous ne détectons pas, et c'est beaucoup plus gênant … !

Nous pensons donc qu'il est nécessaire de limiter autant que possible le recours à des solutions étrangères.

Cette ambition va de pair avec l'élaboration d'une feuille de route pour réduire l'empreinte des GAFAM au sein du ministère des Armées. Nous nous sommes particulièrement intéressés au recours par celui-ci du système d'exploitation Windows. Nous sommes parvenus à la conclusion que le ministère des Armées est aujourd'hui piégé : aucune alternative crédible n'existe à ce système d'exploitation, et le recours aux logiciels libres présente de nombreuses limites, même si l'exploration d'un recours plus accru à Linux nous semble souhaitable.

En outre, compte tenu de l'incapacité actuelle du ministère des Armées à assumer, seul, le maintien en condition de sécurité d'un système d'exploitation alternatif, il est directement tributaire de Microsoft. Ce qui signifie qu'elle est dépendante pour la correction des vulnérabilités informatiques potentiellement exploitées par des acteurs malveillants. Cette dépendance sera d'autant plus grave si, demain, cette entreprise décidait de fournir ses services sur le mode dit de « logiciels en tant que services » (*Software as a Service* (SaaS)).

Ce risque est une véritable épée de Damoclès qui pèse sur la protection des données des services de l'État mais surtout sur notre souveraineté. Cela est dû au fait que le modèle émergent consiste au seul achat de droits d'utilisation de solutions hébergées à l'étranger. D'ailleurs, Microsoft a indiqué que d'ici 2030, voire 2027, il n'y aura plus que des logiciels sous forme de SaaS.

Le ministère des Armées, compte tenu de ses exigences en matière de sécurité et de souveraineté, ne peut accepter cette situation, et aujourd'hui, il est difficile d'estimer l'ampleur des risques…

En outre, la feuille de route du ministère des Armées en matière de défense en profondeur des systèmes d'information doit être poursuivie. Comme entendu en audition, si le ministère a bâti des forteresses, il s'agit désormais de bâtir des villes. Aujourd'hui, il y a un périmètre de sécurité fort autour de l'ensemble des systèmes d'information du ministère.

L'enjeu est d'empêcher que, demain, quelqu'un qui a réussi à pénétrer la forteresse puisse avoir accès à tout. Ce qu'on appelle « la défense en profondeur », dont l'objectif est

d’affiner les portes d’entrée. Cela implique de mieux les sécuriser afin d’empêcher que n’importe quelle personne ait tous les droits d’accès. En fonction, par exemple, de l’identifiant et du lieu de connexion, attribués selon les fonctions occupées au ministère, une personne donnée ne pourra pas avoir accès à l’ensemble des informations qu’elle souhaite, y compris sur la durée, ce qui n’est pas le cas aujourd’hui. Pour cela, il faudrait mettre en œuvre un processus de transition important afin de changer l’architecture numérique du ministère, ce qui ne sera a priori pas le cas avant 2031. Ce que nous regrettons…

**M. Frédéric Mathieu, rapporteur.** Un autre sujet de préoccupation majeur est celui relatif à l’hébergement informatique en nuage. Actuellement, le ministère des Armées met en œuvre une stratégie visant à exploiter tout le potentiel des technologies d’hébergement en nuage. Afin de satisfaire les besoins des systèmes d'information non éligibles à une migration dans des clouds externes, le ministère des Armées développe et exploite plusieurs clouds privés, selon divers niveaux de sensibilité et de classification (non protégé, diffusion restreinte, secret). Des solutions de stockage de données différenciées en fonction des performances attendues sont déployées ou en cours de construction sur ces divers clouds. Cet enjeu a été entamé mais il faut aujourd’hui faire basculer les systèmes d’information un à un sur des systèmes d’hébergement en nuage. Or, le ministère des Armées comprenant plus de 1 500 systèmes d’information, ce processus prendra du temps et on estime que d’ici 2030, entre 50 et 60 % de l’architecture de réseau du ministère seulement aura basculé sur un système de stockage en nuage. Nous estimons qu’il est nécessaire d’accélérer cette feuille de route relative à la migration vers un hébergement informatique en nuage souverain. Nous insistons sur « souverain ». Cet impératif vaut également pour les entreprises de la BITD, les OIV et les OSE, dont les données sont au moins aussi stratégiques que celles des services du ministère des Armées et au-delà.

D’ailleurs, s’agissant, des entreprises de la BITD, nous estimons qu’il est nécessaire de franchir une nouvelle étape pour renforcer leur cyber-résilience, et singulièrement les entreprises de la chaîne de sous-traitance. Lors de nos auditions, il nous a clairement été indiqué que les entreprises de la BITD sont les cibles régulières des cyberattaquants. Plus encore que les rançongiciels, qui frappent aussi les entreprises de la BITD, ce sont les logiciels de cyber-espionnage qui frappent en premier lieu ces entreprises. Il s’agit là d’un enjeu capital : quel est l’intérêt d’investir des milliards d’euros pour se doter de systèmes d’armes performants à même de donner à nos armées une supériorité opérationnelle sur le terrain si les entreprises qui conçoivent ces systèmes d’armes se font piller leurs savoir-faire ? La DRSD est en charge de la sensibilisation des entreprises de la BITD face à ce risque, et notamment le centre de veille et d’alerte dédié aux entreprises de défense créé récemment. Toutefois, nous estimons qu’il est désormais nécessaire d’aller plus loin. C’est pourquoi nous pensons qu’il faudra fixer des critères de cybersécurité aux entreprises de la BITD et à leurs sous-traitants en contrepartie de l’obtention de marchés publics.

Enfin, nous estimons qu’il faudra à l’avenir encadrer de manière très stricte les relations entre le ministère des Armées et les entreprises qui vendent des armes cyber offensives. S’agissant de ses relations avec les *brokers* de vulnérabilités informatiques, la DGA a indiqué que le niveau de confiance envers ceux-ci est extrêmement faible. Il est en effet quasiment impossible de connaître le cycle de vie d'une vulnérabilité ou d’un code exploitant celle-ci ; par exemple : qui l'a trouvé ? à combien de personne il a été vendu ? est-ce qu'il contient des marquants ? Dans le domaine de la LIO, la stratégie de la DGA est donc aujourd’hui de privilégier le recours à des études réalisées par des entreprises de la BITD.

Cette approche permet d'avoir une confiance forte dans les vulnérabilités nécessaires à la réalisation d'armes numériques, car, ce faisant, il n'y a pas de risque d'intoxication et de vente à de multiples acteurs. Nous estimons que cette ligne est la bonne et qu'elle devra être tenue à l'avenir.

**Mme Anne Le Hénanff, rapporteure.** Le cinquième défi porte sur l'innovation et la prospective. Deux domaines en particulier ont retenu notre attention : les technologies quantiques et l'intelligence artificielle.

S'agissant de l'émergence des technologies quantiques, c'est la DGA qui pilote la feuille de route du ministère des Armées :

1/ en finançant des projets de recherche et technologie (R&T) ;

2/ en évaluant la menace que ces technologies, prévisibles ou probables, feront porter sur les systèmes à l'avenir ;

3/ et en développant ses compétences techniques et scientifiques.

Si l'identification des enjeux et la feuille de route semblent claires, nous nous sommes cependant heurtés à la question spécifique de l'ordinateur quantique. Personne n'a été en mesure de nous indiquer si l'avènement de cette nouvelle technologie était imminent, ni si les budgets pour son développement étaient nécessaires !

C'est pourquoi nous estimons indispensable de procéder à une évaluation des coûts, moyens et délais nécessaires à cette nouvelle technologie, ainsi qu'à une estimation de la capacité de la France à s'en doter en propre ou si nous avons besoin d'un partenariat européen pour y parvenir.

Par ailleurs, nous avons été alertés lors de nos travaux sur l'influence croissante de l'intelligence artificielle, et singulièrement de l'intelligence artificielle générative, dans le domaine de la cyberdéfense. Les avancées récentes significatives sont à la fois une opportunité et une menace dans le domaine cyber. Elles peuvent constituer une opportunité notamment pour la LID, par exemple pour l'analyse et la caractérisation de malwares ou la détection de scénarios d'attaque ou la L2I pour aider à détecter des manœuvres informationnelles (par exemple pour l'aide à la formulation de contre-arguments face à une campagne de désinformation).

Un enjeu important, en cas d'utilisation d'IA générative pour la sécurité, est de s'assurer que les données utilisées pour l'apprentissage n'ont pas été empoisonnées, s'assurer de la robustesse et de la qualité des défenses de l'IA. Mais elle peut également constituer une menace dans le sens où elle apporte une capacité décuplée à l'attaquant, notamment dans les domaines de la LIO et de la L2I. Elle peut par exemple aider un attaquant à générer des courriels pour du *phishing*, usurper une identité ou encore simplifier la création d'une cyberattaque, pourtant complexe, (donnant ainsi la capacité à des personnes moins expérimentées d'en créer), d'automatiser des cyberattaques, de générer des fausses informations ou encore de faciliter des attaques informationnelles massives. Or, tous ces apports et toutes ces menaces sont encore exploratoires, quoique plus tangibles que les technologies quantiques. L'élaboration d'une feuille de route relative aux influences

mutuelles entre l'intelligence artificielle générative et la cyberdéfense nous paraît indispensable.

**M. Frédéric Mathieu, rapporteur.** Enfin, le dernier défi est celui de la transparence. Ce défi est avant tout le résultat de notre expérience dans le cadre de notre mission. Le sujet de la cyberdéfense, et singulièrement dans les domaines offensif et informationnel, est d'une sensibilité particulière. Nous avons pu le mesurer lors de nos auditions, au cours desquelles les questions relatives à la LIO et à la L2I se sont très vite heurtées à une absence de réponse compte tenu du fait que les informations relatives à ces deux domaines de lutte informatique sont classifiées et revêtent une sensibilité forte.

Cette précaution peut s'entendre. Mais il n'en demeure pas moins que le défaut de transparence vis-à-vis des Parlementaires que nous sommes sur les activités des armées et des services de renseignement en matière de LIO et de L2I pose question. Si les Parlementaires votent la loi – y compris, donc, les lois de finances –, ils doivent logiquement disposer d'un niveau d'information suffisamment élevé pour pouvoir consentir ou non, de manière éclairée, à l'adoption de dispositions législatives relatives à la politique de cyberdéfense. Or, à l'heure actuelle, ce n'est pas le cas.

Le ministère des Armées a fait un effort de transparence salutaire en 2019 en assumant publiquement de conduire des actions offensives dans le cyberespace. Par ailleurs, si les doctrines de lutte informatique sont classifiées, des éléments publics de doctrine ont été mis à la disposition du grand public, ce qui ne peut qu'être salué. Il n'en demeure pas moins indispensable de franchir une nouvelle étape dans ce domaine, et singulièrement vis-à-vis des Parlementaires, représentants de la Nation. Nous estimons donc nécessaire d'associer davantage le Parlement au suivi de la politique de cyberdéfense du ministère des Armées en matière de LIO et de L2I, et suggérons, pour ce faire, de créer une commission parlementaire chargée du suivi de la politique de cyberdéfense de l'État dont les membres seraient autorisés ès qualités à connaître des informations classifiées relatives à ladite politique.

Voici, chers collègues, les conclusions de nos travaux. Nous nous tenons désormais à votre disposition pour répondre à toutes vos questions.

**M. Mounir Belhamiti (RE).** Au nom du groupe Renaissance, je tiens à vous remercier pour la qualité de votre travail et la pertinence de vos recommandations. Ce n'est sûrement pas un hasard que deux Députés originaires de Bretagne soient mobilisés sur le sujet de la cyberdéfense. Le grand ouest est le fer de lance de la cyberdéfense en France, ce qu'on ne peut que saluer, car cela reflète le dynamisme et la mobilisation de nos territoires.

Des défis, il y en a. Ce domaine est en évolution constante et les menaces de plus en plus sophistiquées. J'imagine les difficultés que vous avez dû éprouver tout au long de vos travaux pour suivre les évolutions dans ce domaine. C'est un champ de conflictualité en tant que tel. La France et l'Europe sont confrontés à des enjeux complexes tels que celui de la coordination des efforts entre les États, le partage efficace des renseignements, la capacité à anticiper et à répondre aux menaces d'origine nationale ou internationale, les lacunes de la collaboration entre les entités publiques et privées, le besoin d'investissement significatif en matière de formation, la question de la régulation des technologies émergentes… autant de défis que vous avez pu dresser. La LPM répond en partie à ce nouveau paradigme car

4 milliards d'euros sont programmés pour la cyberdéfense. Cela s'inscrit dans la démarche d'économie de guerre souhaitée par le président de la République et le ministre des Armées.

Ma question porte sur la prise en compte de critères de cybersécurité applicables aux entreprises de la BITD. Cela concerne évidemment la chaîne de sous-traitants. À votre avis, les marchés publics sont-ils sur ce point à la hauteur des enjeux ? Sommes-nous assez vigilants vis-à-vis des entreprises de la chaîne d'approvisionnement ? Est-ce qu'on accompagne suffisamment ces entreprises ? A-t-on les outils nécessaires pour protéger ces entreprises en cas de crise cyber massive sur le sol français ?

**Mme Anne Le Hénanff, rapporteure.** En préambule, je souhaite préciser que notre cyberdéfense est une cyberdéfense d'excellence. Nous avons pu le mesurer notamment lors de notre déplacement en Finlande et en Estonie. Il y a une vraie admiration pour le modèle de cyberdéfense français.

Les marchés publics sont un vrai frein aujourd'hui, et pas uniquement dans le domaine de la cyberdéfense. On nous dit souvent que la remise à plat des procédures de marchés publics est un travail colossal. Le code des marchés publics est aujourd'hui un obstacle en matière de cybersécurité et de cyberdéfense. Il devrait être possible d'introduire des critères spécifiques liés à l'achat dans le domaine de la cybersécurité. Le code des marchés publics n'est plus adapté à l'environnement et aux nouvelles menaces. La cyber-résilience ne peut passer que par l'accompagnement des acteurs du territoire. Les collectivités achètent les logiciels, et aujourd'hui, la facilité, c'est d'acheter sur étagère. Le code des marchés publics est donc aujourd'hui un vrai frein à la cybersécurité et à la cyber-résilience.

**M. Frédéric Mathieu, rapporteur.** Je ne sais pas si les organisations criminelles ou étatiques qui font du cyber-espionnage sur les entreprises de la BITD ont lu la mythologie grecque mais ils connaissent bien le principe du cheval de Troie, et notamment de porter l'effort sur les entreprises les plus petites et les plus faibles, c'est-à-dire sur les entreprises de la chaîne de sous-traitance. C'est une question qui est bien prise en compte par les gros acteurs de la BITD, qui savent très bien que leurs chaînes d'approvisionnement peuvent présenter des faiblesses.

La fixation de critères de cybersécurité nous semble essentielle. On nous dit que cela induit des coûts supplémentaires pour l'entreprise. Certes, mais c'est peut-être la question du modèle économique de ces entreprises qui doivent prendre en compte, comme coût d'entrée sur un marché, le fait d'être à la hauteur en termes de cyberdéfense. Nous avons espoir qu'une évolution sur le code des marchés publics pourra influencer favorablement les pratiques dans ce domaine et la responsabilisation des acteurs. Le ministère des Armées et l'ANSSI ne peuvent pas arriver systématiquement en secours curatif, au demeurant aux frais du contribuable, pour compenser des moyens qu'une entreprise n'a pas voulu mettre pour garantir sa cybersécurité alors que ses activités sont sensibles. Cela nous a été dit par l'ANSSI, et nous approuvons.

**Mme Caroline Colombier (RN).** Nous souhaitons saluer le travail de grande qualité présenté ce matin, fort de nombreuses auditions menées ces derniers mois.

La cyberdéfense constitue une nouvelle dimension complexe de la conflictualité moderne, impactant tant le domaine civil que le domaine militaire. Face à cela, une mutation psychologique, capacitaire et opérationnelle doit s'imposer. Le développement du numérique

et de l'IA nécessite un renforcement des moyens dévolus à la cyberdéfense. Ainsi, les armées génèrent une masse de données toujours plus conséquente, dont la maîtrise et la protection sont souvent déléguées à des prestataires privés. Or, il est essentiel qu'elle conserve une maîtrise tant de leurs données que de leurs SI dans un intérêt évident de souveraineté. Quelles sont donc vos pistes de réflexion pour aider nos armées à reprendre la main sur leurs SI ?

Par ailleurs, nous souhaitons recueillir votre avis sur la crise actuelle que traverse l'entreprise Atos. Endettée de plus de 5 milliards d'euros, cette entreprise doit en rembourser la moitié avant 2025. Ces derniers jours, son action a totalement plongé. Atos est non seulement un prestataire technologique de premier ordre dans le cadre des JOP 2024, mais elle joue également un rôle essentiel dans notre dissuasion dans la mesure où elle fournit les supercalculateurs nécessaires aux simulations d'essais nucléaires. Or, pour renflouer sa dette, Atos souhaite vendre sa branche « cybersécurité et infogérance ». Cette crise traversée par ce fleuron français vous inquiète-t-elle ? Quelles mesures envisageriez-vous pour la remettre à flots afin qu'il poursuive le rôle qu'il occupe depuis 1997 dans la défense et la souveraineté nationale ?

**Mme Anne Le Hénanff, rapporteure.** S'agissant des SI des armées, le ministère des Armées travaille beaucoup sur ce sujet dont ils ont conscience. Ceci dit, s'agissant, par exemple, de Linux, on nous a aussi indiqué qu'en l'état, il n'était pas possible de transposer les SI utilisés aujourd'hui sur Windows vers Linux en peu de temps – cela demanderait des années – et par ailleurs, il faudra travailler sur Linux, car il ne pourrait pas être mis en place en l'état. Il faudrait donc conduire des travaux de sécurisation, ce qui induira un coût et prendra du temps. Mais le ministère des Armées a bien conscience de cette dépendance. On nous a aussi indiqué que ces SI sont utilisés dans des domaines non-sensibles, et qu'à partir du moment où des actions sont considérées comme sensibles ou secrètes, il y a, au sein des armées, les compétences et l'expertise qui permettent de sécuriser les SI et éviter l'intrusion par des personnes extérieures dans des domaines que les armées ne souhaitent pas rendre accessibles ; et heureusement ! Il y a plusieurs cercles concentriques : un premier cercle pour le tout-venant, un cercle plus fermé, et un cercle très fermé. Mais cela ne retire rien à notre constat.

**M. Frédéric Mathieu, rapporteur.** S'agissant d'Atos, vous avez décrit la situation de l'entreprise. Ce sujet mériterait en réalité une commission d'enquête. Que dire ? Nous avons un fleuron industriel, qui est l'héritier de l'engagement de la France de longue date dans le domaine de l'informatique et des technologies de communication. Nous sommes très préoccupés par la question de la souveraineté, notamment pour les matériels informatiques. L'exemple d'Atos ne fait que confirmer la nécessité que l'État redevienne un État stratège dans ce domaine. Des députés ont déposé des amendements sur le PLF pour nationaliser Atos de manière provisoire et préventive. J'ai moi-même déposé une PPL pour que l'État participe durablement au capital d'Atos. Je ne vais pas faire la publicité de ma PPL ! Mais cette question nous préoccupe tous. Au-delà d'Atos, la question en filigrane est celle de la vision stratégique de l'État : est-ce que la France peut se permettre d'être dépouillée de nos capacités industrielles ? J'espère que nous arriverons à faire comprendre dans le débat public que le numérique n'est plus une simple fonction support : c'est devenu une fonction stratégique, qui peut être une arme en soi. Le sentiment que nous avons aujourd'hui, c'est que cela n'est pas bien pris en compte en termes de vision stratégique.

**M. Aurélien Saintoul (LFI-NUPES).** Votre travail a un mérite particulier : il est quasiment exhaustif. Je dis « quasiment » car il met un peu de côté la question de la dissuasion, au sujet de laquelle personne ne vous donnera de réponses dans le domaine de la défense. Mais je pense qu'il faut avoir à l'esprit que la question de la cyberdéfense dans le domaine de la dissuasion devra nous faire réfléchir. Je n'en dirai pas davantage, mais nous devons connecter ces deux sujets. Je me permets de répondre à notre collègue Mounir Belhamiti, qui a évoqué le fait que la LPM répond « en partie » aux défis de la cyberdéfense : répondre en partie aux défis, c'est ne pas y répondre.

Néanmoins, je note que votre rapport dresse l'ensemble des perspectives et montre qu'il y a un enjeu de dépendance extrêmement fort. Il n'y a pas d'autre façon d'y répondre qu'en ayant une ambition à la hauteur des enjeux. J'entends dans votre travail des choses qui consonnent énormément avec le programme de La France insoumise, et singulièrement avec la valorisation que nous accordons à la notion de planification, ce dont je me réjouis.

Vous avez évoqué le quantique. Vous suggérez un audit de nos politiques. Avez-vous quand même un aperçu de la stratégie mise en œuvre jusqu'à présent ? Avez-vous perçu une cohérence dans l'appréciation que l'État a de ce sujet ? Ou avez-vous eu le sentiment d'une approche plutôt impressionniste ?

Ensuite, s'agissant des ressources humaines, qui sont un des grands défis, est-ce qu'une école comme Polytechnique fournit les contingents nécessaires ? Ou pourrait-on faire mieux ? D'autres écoles pourraient être mobilisées, mais s'agissant de Polytechnique, nous avons peut-être un sujet la concernant.

J'avais également une question sur Atos, à laquelle vous avez globalement répondu, qui portait sur l'idée que c'est en réalité l'ensemble de l'écosystème qui devrait être consolidé. C'est notre conviction. Nous manquons de profondeur de vue si nous ne savons pas que Atos a sauvé Bull, et que Bull était pourtant public et qu'il a été privatisé. C'est peut-être l'ensemble de ces mouvements de capitaux et de ces stratégies erratiques au fil des années que nous devrions interroger.

Enfin, la dernière question porte sur la L2I. Avez-vous pu avoir des éléments tangibles sur les restrictions éthiques que nous appliquons ? C'est une question que je pose souvent. Avez-vous pu rentrer dans la machine ?

**M. Frédéric Mathieu, rapporteur.** S'agissant de la L2I, c'est compliqué de rentrer dans la machine, comme vous dites ! Il s'agit d'un domaine très sensible. On sait que les armées mènent des actions dans le champ informationnel. Mais il s'agit d'informations classifiées. Cela est en rapport avec notre proposition de créer une commission *ad hoc*, qui permettrait à une délégation de notre assemblée d'avoir une vision claire sur ce sujet, selon les mêmes modalités et le même type de fonctionnement que la DPR.

S'agissant du quantique, on nous dit qu'il faut lancer des études sérieuses sur la question. Je vais vous confier une anecdote sans vous dévoiler les acteurs concernés. En l'espace d'une matinée, au sujet de la dotation par l'État d'un ordinateur quantique, on a rencontré deux hauts décideurs qui auraient dû avoir les idées claires sur cette question. Lors de la première audition, on nous a dit que les investissements nécessaires pour se doter d'un ordinateur quantique seraient très élevés. Lorsqu'on a demandé combien, on nous a indiqué que cela coûterait au moins 100 millions d'euros. Pourtant, 100 millions d'euros, ce n'est pas

si cher… et au même moment, nous apprenions que le surcoût du projet immobilier de la DGSE au Fort Neuf de Vincennes était de 185 millions d'euros… lors de la seconde audition, nous avons reposé la question. La personne que nous auditionnions nous a dit que le coût afférent était tellement élevé qu'on ne peut pas le chiffrer. Donc, dans la même matinée, nous avons eu une fourchette allant de 100 millions d'euros à l'infini en dilatation constante… on est dans le quantique cela dit, donc on passe de l'infiniment petit à l'infiniment grand !

Plus sérieusement, cela est triste car nous sommes persuadés qu'il y a des gens au sein des services qui savent très bien ce qu'il en est car nous avons la capacité en interne de faire ce type d'évaluations. Mais ce que cette anecdote montre, c'est qu'il y a deux options : soit l'information ne remonte pas au bon niveau, soit on ne se pose pas la question en haut lieu. Cela m'inquiète quant aux conseils politiques prodigués aux grands décideurs politiques. On préconise donc la conduite d'une étude pour connaître le coût, les délais et les partenaires européens éventuels avec lesquels cela pourrait être fait.

J'ai le sentiment que, s'agissant du quantique, on est à une époque similaire à celle du milieu des années 1930 avec l'atome : on sait que ça existe, on sait qu'il y a des potentialités, on sait qu'on pourrait en faire une arme… mais tout cela, on ne le saura que si on décide de se lancer dans le Projet Manhattan. Aujourd'hui, la France et l'Europe en sont à ce point-là. Il faut donc travailler ce sujet. Si le quantique s'affirme comme une réalité dans les années qui viennent, on est face à quelque chose en potentiel offensif qui est de l'ordre de la dissuasion nucléaire. La question est donc de savoir si on veut passer à côté ou non.

**Mme Anne Le Hénanff, rapporteure.** Sur les ressources humaines, nous ne sommes jamais mieux servis que par soi-même. Le partenariat entre l'École Polytechnique et l'EPITA a l'avantage de répondre aux besoins. La première promotion ne sera que de 30 étudiants, mais c'est un bon début. La conclusion de partenariats entre le ministère des Armées et des écoles d'ingénieurs ou la création de BTS et d'IUT a l'avantage d'aboutir à des formations adaptées aux besoins du ministère des Armées. Nous croyons également à une approche sectorielle dans ce domaine, en adaptant la formation aux besoins des armées. C'est ce vers quoi le ministère des Armées tend. Mais cela ne suffira pas : il faudra aller plus loin. Le COMCYBER est pleinement engagé dans cette voie.

S'agissant de la L2I, les armées agissent dans un cadre déontologique national et international : ils ne font pas n'importe quoi ! Il y a un cadre, et la démarche est essentiellement défensive dans le domaine informationnel. Lorsque des vagues de désinformation en provenance, par exemple, du Sahel, il s'agit de rectifier ces fausses informations, en prouvant leur caractère fallacieux. On ne fait pas de la désinformation gratuite ou des actions pour décrédibiliser des États.

**M. Jean-Louis Thiériot (LR).** Je tiens à vous dire à quel point votre exposé était absolument passionnant, clair et surtout très pédagogique. Pour quelqu'un qui ne vient pas forcément de ce secteur, c'était d'une clarté exceptionnelle. Je tenais à vous en remercier.

Vous nous avez présenté l'architecture et la doctrine française. Avez-vous procédé à des comparaisons internationales ? Quelle est la doctrine de l'OTAN en termes de cyberdéfense ? Enfin, des leçons de la guerre en Ukraine peuvent-elles être tirées en matière de cyberdéfense ? La question du quantique est majeure. J'ai beaucoup aimé votre référence à

la rupture épistémologique potentielle entre l'atome et le quantique. Que font nos compétiteurs stratégiques ?

Ensuite, s'agissant du SaaS, c'est un sujet de préoccupation qui m'inquiète beaucoup depuis très longtemps. Quelles solutions pourrait-on avoir à moyen terme et à quels coûts ? Et comment ferait-on pour la dissuasion ? J'ai la faiblesse de croire, s'agissant de la dissuasion, qu'on a réussi à élaborer une architecture numérique totalement souveraine.

Enfin, le COMCYBER n'est-il qu'un commandement opérationnel ? Si oui, existe-t-il par ailleurs un commandement organique ?

**Mme Anne Le Hénanff, rapporteure.** S'agissant du SaaS, les armées ne pourront pas répondre seules à ce défi. C'est logique, car cette problématique concerne tous les ministères sans exception. Ce ne sont pas aux armées de trouver des solutions. Les échanges que nous avons eus nous prouvent qu'ils ont conscience de cela. À l'échelle interministérielle, c'est la DINUM qui est responsable. La solution ne pourra venir que du plus haut niveau, y compris à l'échelon politique, et en l'occurrence, celui du Premier ministre. C'est à lui de s'emparer de ce sujet. Cela étant dit, exclure tous les logiciels extraterritoriaux, ce n'est pas sérieux. Il faut trouver un juste équilibre, ce qui prendra du temps mais nous devons nous y atteler au plus haut niveau de l'État, qui est celui du Premier ministre. Nous devons nous emparer de ce sujet.

S'agissant des comparaisons internationales, la sensibilité à la cyberdéfense et à la cybersécurité est très loin de ce qu'on a pu constater en Finlande et en Estonie. Pour nous, ce sont des modèles. Pourquoi ? L'Estonie est vraiment la référence en matière de numérique, car ils ont franchi une étape sur l'identité numérique du citoyen que nous n'avons pas encore franchi. Nous avons été impressionnés dans ces deux pays par le fait que dès l'école primaire, les élèves entendent parler d'hygiène numérique ou de désinformation. Les enfants sont parties prenantes de la cyber-résilience dans ces pays. En France, ce que nous constatons, c'est que la cybersécurité est un sujet d'experts, très fermé. Avec ce rapport, nous souhaitons que ce sujet s'ouvre à la nation tout entière. La révision de la Revue stratégique de cyberdéfense en cours peut être l'occasion d'aller plus loin.

S'agissant de l'Ukraine, la Finlande et l'Estonie sont en cyber guerre. Ils subissent régulièrement des cyberattaques depuis le déclenchement de la guerre en Ukraine. Nous avons des leçons à tirer de cela. Mais ils sont aussi demandeurs vis-à-vis de la France, notamment en matière d'exercices. On a donc beaucoup à apprendre d'eux, mais ils sont aussi en attente vis-à-vis de nous.

**M. Frédéric Mathieu, rapporteur.** Le COMCYBER assure à la fois un commandement organique et un commandement opérationnel. Toutefois, avec la création de la communauté cyber des armées, l'objectif est bien de donner des marges de manœuvre aux armées sur les échelons tactique et opératif, sous le contrôle du COMCYBER.

Sur la guerre en Ukraine, beaucoup d'aspects sont confidentiels. Mais notre recommandation sur la nécessité de réfléchir au cadre juridique du mercenariat cyber est liée aux enseignements que nous avons pu tirer de la guerre en Ukraine. La nécessité de conduire des exercices en situation réelle est également un autre enseignement de la guerre en Ukraine.

S’agissant du quantique à l’étranger, les États-Unis et la Chine sont les deux acteurs les plus en avance. Mais peu d’informations circulent. Quand on a évoqué le sujet du quantique avec des autorités nationales, on nous a indiqué qu’on ne pourra rien faire sans le secteur privé, notamment pour des raisons de coûts. De notre point de vue, il faudra s’émanciper de réflexes dogmatiques car lorsqu’on nous a parlé d’une nécessaire participation du secteur privé qui devra avoir l’assurance qu’il pourra exporter la technologie quantique, dont on ne connaît pas encore les implications, on a toussé ! Or, comme je le disais en audition, je n’ai pas le souvenir que le général de Gaulle ait fait un appel à projets sur les marchés financiers pour la dissuasion nucléaire… ce qui donnait lieu à un silence poli, mais gêné ! Il faut donc avancer et aller à un niveau de maturité supérieure s’agissant du quantique. On ne peut pas rester dans le niveau d’obscurité actuel.

**M. Christophe Blanchet (Dem).** Je vous remercie sincèrement pour votre exposé vivant, passionnant, éduquant mais très inquiétant !

S’agissant de l’organisation de la cyberdéfense en millefeuilles, j’ai l’impression qu’on s’y perd rapidement… et il ne s’agit que d’une version simplifiée ! Est-ce que la gouvernance de la cyberdéfense ne serait pas plus performante si, comme pour les millefeuilles administratifs, on opérait quelques coupes ?

Par ailleurs, vous avez parlé des cyberattaques mais vous avez élargi à l’ensemble de la population. Avez-vous quantifié le nombre de cyberattaques que la France a subies ? Cela me semble important de quantifier la menace pour embarquer la population dans cette démarche de cyber-résilience.

Pendant votre intervention, j’ai pu voir le nombre de personnes à proximité sur WhatsApp. Il y avait 10 profils chinois connectés à moins de 500 mètres d’ici. Quel regard portez-vous sur les applications telles que Telegram et WhatsApp ? Est-ce que Tchap est une solution viable ?

Enfin, comment ne pas parler des réserves ? Vous avez évoqué les réservistes opérationnels dans votre propos. Je suis d’accord pour dire qu’il faudrait davantage de réservistes opérationnels. Mais s’agissant des réservistes citoyens, c’est une manne utile et nécessaire. Comment la politique de défense nationale s’opère-t-elle à ce sujet ? Est-ce qu’il y a une ambition ? Lors des débats sur la LPM, nous avions vu qu’il n’y avait pas de compréhension sur l’utilité de la réserve citoyenne. Pourtant, il s’agit de personnes passionnées qui pourraient transmettre ces messages sur la cybersécurité, notamment dans les écoles.

**Mme Anne Le Hénanff, rapporteure.** La réserve citoyenne est un sujet stratégique pour la cyberdéfense. C’est un sujet utile et indispensable car il contribue au renforcement du lien armées-Nation ! On a un objectif sur la réserve opérationnelle. Ces réservistes opérationnels jouent un rôle stratégique pour la cyberdéfense française. Mais s’agissant de la réserve citoyenne dans le domaine de la cyberdéfense, sujet dont j’ai souvent parlé avec le COMCYBER, elle a existé. Il y a une volonté de la remettre en œuvre. C’est vrai que la priorité était la réserve opérationnelle. La réserve citoyenne est plutôt active avec la Gendarmerie. Il y a aussi des réservistes dans la Police nationale. Il y en a moins dans les armées. Je formule le vœu qu’on réarme – si je puis dire ! – les armées en réservistes citoyens car ceux-ci ont des vraies compétences. La volonté de redéployer la réserve citoyenne fait

partie des ambitions des armées, et nous serons là pour les accompagner dans l'atteinte de cet objectif.

S'agissant du millefeuille, il ne faut couper aucune compétence. Mais on a un point majeur : au niveau de la gouvernance, il faudra réorganiser la cyberdéfense en France. L'organisation est encore trop silotée. Il y a des chasses gardées, ce qui est inacceptable. Par ailleurs, cette organisation est trop pyramidale : du haut vers le bas. Nous pensons au contraire que l'organisation de la cyberdéfense doit être transversale.

**M. Frédéric Mathieu, rapporteur.** Nous vous avions présenté la version simplifiée de l'organisation de la cyberdéfense, mais l'organisation est en réalité beaucoup plus complexe, comme le soulignait notre collègue Mounir Belhamiti.

**M. Mounir Belhamiti (RE).** Et il n'y a même pas de ministre !

**Mme Anne Le Hénanff, rapporteure.** C'est vrai !

**M. Frédéric Mathieu, rapporteur.** Tout à fait. La question de la création d'un ministère chargé de la cybersécurité est d'ailleurs régulièrement évoquée dans les cercles qui réfléchissent à la réorganisation de cette politique. En tout cas, force est de constater que chaque service s'est doté de ses capacités propres. La création de la communauté cyber des armées va dans le bon sens. Mais nous sommes attachés au *continuum* de cybersécurité et de cyber-résilience de la Nation. On ne va pas pouvoir rester très longtemps dans le modèle actuel, et tant pis si cela heurte certains conservatismes dans certaines administrations publiques : il va falloir avoir une approche globale. Si cette ambition arrive à maturité, il y aura des changements dans l'organigramme. Mais comme le disait ma collègue, on ne peut pas couper des compétences.

S'agissant des messageries cryptées, nous savons qu'il y a un sujet. On ne sait pas ce qu'il en est spécifiquement pour chaque application, mais au sein des armées, des consignes sont passées pour sensibiliser au risque encouru par le recours à des messageries au quotidien, même lorsqu'elles prétendent être parfaitement cryptées.

Enfin, s'agissant du nombre de cyberattaques, il y a des statistiques dans les rapports d'activité de l'ANSSI. Toutefois, il ne s'agit que des cyberattaques connues : il y a des cyberattaques qui ont pu toucher la France au sujet desquelles aucune publicité n'est faite pour des raisons évidentes de confidentialité.

**Mme Mélanie Thomin (SOC).** Au nom du groupe Socialistes et apparentés, je vous remercie pour ce rapport qui est force de propositions et qui fait honneur à l'audace du travail parlementaire. Bravo à tous les deux !

Nous partageons le fait que l'anticipation et la lutte contre les menaces cyber sont primordiales dans notre approche des conflits modernes et doivent être un élément structurant de notre politique de défense nationale. Les attaques cyber sont discrètes et ont une portée sans limite, comme vous l'avez très bien dit. Nos services publics et l'économie du pays sont devenus des cibles de choix.

S'agissant du travail parlementaire qui pourrait émerger en réaction à votre rapport, ma première question portera sur les logiciels. Pour reprendre votre raisonnement concernant

les logiciels en tant que service, comment peut-on encadrer juridiquement cette pratique pour contrer leur expansion ? Pourrait-on, par exemple, contraindre par la loi chaque éditeur de logiciel proposant un logiciel en tant que service par abonnement à obligatoirement proposer une version sous licence propriétaire ?

Par ailleurs, s'agissant de l'IA générative, un aspect intéressant soulevé dans la LIO et la L2I est que les cyberattaques peuvent avoir pour cibles des bases de données. Comment garantir la protection de ces bases de données ? Faudrait-il imposer aux éditeurs un stockage physique en France ou *a minima* en Europe ?

**M. Frédéric Mathieu, rapporteur.** S'agissant de l'IA générative, il faut avoir en tête que la localisation géographique n'est pas un critère pertinent. Les règles d'extraterritorialité de certains États, notamment des États-Unis, sont telles que le fait d'avoir un serveur de Microsoft sur le sol français ne prémunit en rien de toute ingérence du département d'État américain sur nos données. La question n'est donc pas celle de la localisation géographique. Il s'agit d'un sujet de conflits de lois, entre la loi nationale et la loi extraterritoriale.

S'agissant du travail parlementaire, le rapport vous appartient désormais ! Ce n'est plus uniquement notre œuvre. On peut imaginer beaucoup de choses. L'acquisition de logiciels sous licence propriétaire peut s'étudier mais elle ne réglera pas la question des portes dérobées dès lors que ce logiciel n'est pas souverain. L'enjeu est de se prémunir de la mise en place de portes dérobées. On peut tout à fait acheter un système propriétaire et en être victime. On a ressenti un malaise lorsqu'on évoquait le sujet de Windows. En insistant, on finissait par nous répondre que les Américains sont nos alliés. Pourtant, ce sont ceux qui nous ont le plus espionnés ces dernières années… en tout cas de manière connue. *A contrario*, on nous a dit que l'État est propriétaire de ces logiciels et que, par conséquent, il a la main dessus. Je répondais systématiquement à cet argument que le recours à des matériels ou à des logiciels chinois comme Huawei ne posait donc aucun problème ; et là, on nous disait que si, cela posait problème, et les raisons invoquées s'appliquaient en réalité totalement à Microsoft. Donc, en effet, la question est d'avoir des solutions souveraines sur lesquelles on a pleinement la main.

**Mme Anne Le Hénanff, rapporteure.** Avec mon collègue, nous n'avons jamais travaillé dans l'optique d'un travail législatif. Nous avons vécu cette mission. Désormais, nous partageons nos conclusions. Nous avons nos recommandations mais nous n'avions pas d'objectif législatif.

S'agissant de la protection de notre souveraineté, je crois beaucoup au travail de l'Europe. On a voté le projet de loi « sécuriser et réguler l'espace numérique » à l'Assemblée nationale. L'IUCS permettra de fixer le niveau de cybersécurité imposé en Europe. L'ANSSI est très impliquée à ce sujet. On souhaite que la France donne le ton quant au niveau de cybersécurité exigé en Europe. J'espère qu'on atteindra cet objectif. L'examen à venir de la directive NIS 2 permettra aussi de renforcer notre cybersécurité.

Enfin, comme mon collègue l'a dit, la localisation géographique des serveurs n'entre pas en ligne de compte. Ce qui compte, c'est la cybersécurité et l'extraterritorialité. Pour vous rassurer, le ministère des Armées détient en propre son centre de données.

**M. Loïc Kervran (HOR).** Je remercie nos deux co-rapporteurs et saluer quelques points qui me semblent importants. L'importance de votre travail est perceptible dans la

qualité du rendu. L'expérience de Mme Le Hénanff, en tant qu'élue locale, se reflète aussi dans vos travaux et préconisations. Je salue aussi votre bonne entente et votre capacité à dépasser les différences politiques, ce qui est toujours le cas, du reste, dans cette commission. Votre approche globale qui dépasse les seules armées mais qui s'inscrit bien dans l'approche de défense nationale augure de l'orientation des travaux de la commission cette année sur les aspects de défense et de résilience nationale. C'est une excellente manière de rentrer dans cette phase.

S'agissant de la gouvernance, je salue vos objectifs pour améliorer la lisibilité et l'approche globale de la cybersécurité et de la cyberdéfense. Sur le partage des savoir-faire des armées, jugez-vous que les armées ont des marges de manœuvre, notamment en termes d'effectifs et de temps, pour partager ces savoir-faire vers le civil ?

Vous évoquez les effectifs du CERT de l'ANSSI. Avez-vous une idée du nombre d'ETP supplémentaires nécessaires ?

Enfin, vous évoquez votre souhait de créer une commission parlementaire sur la cyberdéfense. Est-ce que vous jugez que la DPR ne s'intéresse pas assez à ces questions de cyberdéfense ? Vous avez évoqué l'importance du rôle des services de renseignement dans ces questions. Comme vous le savez, les Parlementaires de la DPR sont habilités ès qualités et ont produit des travaux sur la cyberdéfense. Où est la marge de progrès ? Est-ce que la création d'une commission supplémentaire se justifie pour compléter les travaux de la DPR ?

**Mme Anne Le Hénanff, rapporteure.** S'agissant de la gouvernance et du partage des savoir-faire des armées, il faut avoir à l'esprit que les militaires sont vraiment des acteurs d'excellence en France sur le sujet de la prévention, de la sensibilisation, jusqu'à la gestion de crise et la remédiation. L'idée n'est pas de faire intervenir les militaires dans le civil, à la demande, lors d'actions ou de crise cyber. Mais nous trouvons dommage qu'il n'y ait pas davantage de partage de pratiques, de feuille de route, de mode d'emploi de leurs capacités et de leur savoir-faire. Il faut un intermédiaire entre les militaires et le secteur civil pour diffuser et mettre en œuvre ces bonnes pratiques. Prenons l'exemple d'un exercice cyber. Comment une commune de plusieurs dizaines de milliers d'habitants doit réagir pour éviter la diffusion d'une cyberattaque ? La conduite d'exercices peut y aider, et dans ce domaine, les militaires sont les plus compétents.

**M. Frédéric Mathieu, rapporteur.** S'agissant de la spécificité d'une commission, tout le renseignement n'est pas contenu dans le cyber et tout le cyber n'est pas contenu dans le renseignement. La DPR est une commission ad hoc sur la politique de renseignement, mais même si les domaines peuvent se superposer, ils ne se confondent pas totalement. Après, si, dans plusieurs années, après avoir mis en place cette commission, on estime qu'il faudra mettre en place une commission plus large, en plus de la DPR et de la CNCTR, on pourra avoir ce débat. À notre sens, le sujet est celui de la visibilité et de la transparence. En termes de fonctions de contrôle parlementaire, il faut pouvoir être tenu informé des opérations conduites dans le cyberespace et dans le champ informationnel.

S'agissant du CERT de l'ANSSI, nous ne sommes pas en mesure de donner une estimation précise du nombre d'ETP nécessaires pour, par exemple, armer l'ANSSI pour garantir la cybersécurité des DROM-COM. Mais cela pourrait être le cas dans le cadre de futurs travaux parlementaires.

**M. José Gonzalez (RN).** Je vous remercie pour votre travail. Le CEMAT indiquait récemment que l'IA ne changera pas la nature de la guerre. Or, l'usage de l'IA dans le domaine de la cyberdéfense s'intensifie. Le conflit actuel en Ukraine l'a bien mis en lumière. Les Ukrainiens utilisent les moyens cyber pour rattraper leur retard sur les Russes. Le général Grégoire de Saint-Quentin, ancien commandant des forces spéciales, semble adopter la même ligne que le CEMAT. Au regard des auditions que vous avez menées, partagez-vous cet avis ? Ou pensez-vous au contraire que l'IA bouleversera la nature des conflits modernes ? Est-ce simplement un outil complémentaire aux outils existants ? Enfin, quelle stratégie la France doit-elle adopter pour s'adapter aux nouveaux défis de l'IA et l'intégrer pleinement à notre stratégie de défense ?

**Mme Murielle Lepvraud (LFI).** Pensez-vous que la montée en compétences progressive de l'ANSSI pourrait amener à combler le recours au secteur privé ? Si oui, à quelle échéance ? Les protocoles de contrôle assurent-ils la protection des données auxquelles ces entreprises privées ont accès dans le cadre de leurs missions ?

**Mme Anne Le Hénanff, rapporteure.** L'IA ne va pas modifier la forme des conflits. Mais la maîtrise et l'indépendance de l'IA nous conféreraient une supériorité opérationnelle. L'IA n'est qu'un moyen pour mieux anticiper et mieux connaître nos adversaires, et s'agissant de la L2I, de mettre en œuvre des actions qui nous positionneraient dans une situation de maîtrise et d'avance par rapport à nos adversaires.

**M. Frédéric Mathieu, rapporteur.** S'agissant des entreprises privées, l'ANSSI intervient en propre lorsque les crises cyber sont suffisamment critiques. La plupart des temps, en effet, elle a recours à des prestataires privés agréés. La question de la confidentialité des données auxquelles peuvent avoir accès ces entreprises privées se pose en effet. Mais nous estimons que le droit pénal suffit à encadrer ce risque. La question qui peut se poser en revanche est celle de la nature très diverse des interventions qui peuvent avoir lieu. On est bien obligés d'agréer des entreprises privées selon un cahier des charges, mais cela ne nous dit rien de la rigueur du cahier des charges, tout comme cela ne nous dit rien des contrôles mis en œuvre au long cours pour s'assurer du respect du cahier des charges. Je ne remets pas en cause la rigueur de l'ANSSI pour effectuer ces contrôles, mais il y a un défi capacitaire : il faut bien avoir des entreprises qui puissent intervenir sur place en cas de besoin. On se doute bien qu'il faut s'adapter aux réalités du terrain : on ne peut pas placer un niveau d'exigence trop élevé, sinon, on n'agrée personne. C'est davantage sur cette mécanique que les préoccupations doivent porter.

**M. le président Jean-Pierre Cubertafon.** Bravo à nouveau à nos deux collègues pour la très grande qualité de leur travail. Nous allons donc désormais procéder au vote pour autoriser la publication du rapport.

*La commission **autorise** le dépôt du rapport d'information sur les défis de la cyberdéfense.*

*

* *

*La séance est levée à onze heures quarante.*

*

*  *

**Membres présents ou excusés**

*Présents.* - M. Jean-Philippe Ardouin, M. Mounir Belhamiti, M. Pierrick Berteloot, M. Christophe Blanchet, M. Frédéric Boccaletti, M. Hubert Brigand, M. Vincent Bru, Mme Caroline Colombier, M. François Cormier-Bouligeon, M. Jean-Pierre Cubertafon, Mme Martine Etienne, M. Yannick Favennec-Bécot, M. Jean-Marie Fiévet, Mme Anne Genetet, M. Frank Giletti, M. Christian Girard, M. José Gonzalez, M. Jean-Michel Jacques, M. Loïc Kervran, Mme Anne Le Hénanff, Mme Gisèle Lelouis, Mme Patricia Lemoine, Mme Murielle Lepvraud, Mme Jacqueline Maquet, Mme Pascale Martin, Mme Michèle Martinez, M. Frédéric Mathieu, M. Pierre Morel-À-L'Huissier, M. Christophe Naegelen, Mme Valérie Rabault, M. Julien Rancoule, M. Aurélien Saintoul, Mme Isabelle Santiago, Mme Nathalie Serre, M. Philippe Sorez, M. Bruno Studer, M. Michaël Taverne, M. Jean-Louis Thiériot, Mme Mélanie Thomin, Mme Corinne Vignon

*Excusés.* - Mme Valérie Bazin-Malgras, M. Christophe Bex, M. Benoît Bordat, Mme Yaël Braun-Pivet, M. Steve Chailloux, Mme Cyrielle Chatelain, M. Emmanuel Fernandes, M. Thomas Gassilloud, M. Bastien Lachaud, M. Sylvain Maillard, M. Olivier Marleix, Mme Lysiane Métayer, Mme Anna Pic, M. François Piquemal, Mme Josy Poueyto, Mme Natalia Pouzyreff, Mme Marie-Pierre Rixain, M. Fabien Roussel, M. Mikaele Seo, Mme Sabine Thillaye