ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition, à huis clos, de M. le général de division Aymeric Bonnemaison, commandant de la cyberdéfense, sur le projet de loi de programmation militaire pour les années 2024 à 2030.

Jeudi
13 avril 2023
Séance de 11 heures

Compte rendu n° 64

SESSION ORDINAIRE DE **2022-2023**

Présidence de M. Thomas Gassilloud, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures cinq.

M. le président Thomas Gassilloud. Mes chers collègues, nous auditionnons le général Aymeric Bonnemaison, commandant de la cyberdéfense (Comcyber), dans le cadre des travaux préparatoires à l'examen du projet de loi relatif à la programmation militaire pour les années 2024 à 2030, qui accorde 4 milliards d'euros au cyber et en fait une priorité pour nos armées.

En votre qualité de Comcyber, vous serez donc amené, mon général, à jouer un rôle central. Chacun a bien compris, désormais, l'articulation de notre dispositif cyber. L'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont nous avons auditionné le nouveau directeur général la semaine dernière, est le bouclier ; le Comcyber est le glaive.

Nous aimerions vous entendre dire comment vous comptez utiliser les crédits en hausse dédiés au cyber pour les sept prochaines années, et préciser l'état de la menace cyber, ainsi que la manière dont la loi de programmation militaire (LPM) 2024-2030 permettra d'y faire face.

Général Aymeric Bonnemaison, commandant de la cyberdéfense (Comcyber). C'est la deuxième fois que je m'exprime devant vous et la troisième fois que je viens ici depuis ma prise de fonction en septembre. Cela démontre toute l'importance prise par le fait cyber, ce dont je me réjouis en tant que Comcyber.

Précédemment, j'ai abordé le bilan de la LPM 2019-2025 sous l'angle cyber et présenté mon analyse des enseignements de la guerre en Ukraine. Ces deux thèmes constitueront le socle de mon propos, car ils ont servi de base à nos travaux sur la future LPM et à nos demandes.

Je commencerai par rappeler les éléments d'appréciation dont nous disposons sur la menace cyber, tant ce qu'elle est que ce qu'elle pourrait devenir. Je présenterai ensuite les grandes orientations de la réponse apportée par la LPM 2024-2030, et enfin notre dynamique interne d'organisation et d'optimisation compte tenu des éléments dont nous disposons et des moyens dont nous allons être dotés.

L'état de la menace cyber vous a sans doute été en partie présenté par le directeur général de l'ANSSI. La menace générale est toujours croissante, plus complexe et sans cesse renouvelée. Elle est plus connue qu'il y a une dizaine d'années, lorsque nous commencions à l'appréhender, notamment parce que certaines collectivités locales ont été, hélas, la cible de ce type d'attaques.

Ces attaques sont de trois ordres. Certaines relèvent de l'espionnage. Ce sont celles dont on parle le moins, car elles restent sous le radar et attaquent le plus souvent le monde économique et industriel, parfois des particuliers. D'autres visent à la subversion et à la déstabilisation à partir des réseaux sociaux. Elles sont bien plus visibles. Nous les affrontons, notamment en Afrique francophone, mais tout le monde y est exposé. Des élections américaines et françaises ont été perturbées par ce type d'action par le passé. Les autres attaques sont les fuites et les ventes de données sensibles, ainsi que les sabotages, qui entraînent des dysfonctionnements.

Parmi les tendances des dernières années, il faut relever le développement d'attaques systémiques importantes. Certes, le conflit ukrainien n'a pas mis à genoux l'État ukrainien, mais plusieurs attaques survenues en 2022 méritent d'être mentionnées. En avril 2022, une attaque par rançongiciel a contraint le Costa Rica à déclarer l'état d'urgence, notamment parce que le système de santé et les systèmes financiers étaient au tapis. L'Albanie et le Monténégro ont signalé des attaques majeures, qu'ils ont attribuées à des puissances étrangères.

Depuis 2019, les attaques par rançongiciel se développent. Elles agissent sur deux plans : chiffrer les données et les rendre inaccessibles, ce qui neutralise le système ; les extraire et les revendre. Cette double extorsion tend à se développer : dans la mesure où de plus en plus de sociétés font des sauvegardes de leurs données, elles paient moins pour les récupérer que pour en éviter la divulgation par les cybercriminels.

Les acteurs sont insaisissables et entremêlés – États, services de renseignement, criminels, activistes.

Les modes d'attaque présentent une sophistication croissante. Les armes cyber se disséminent, non seulement sur le *dark web*, mais aussi par l'action de sociétés proposant le hacking comme un service, telles que NSO Group (Pegasus). Les attaques de la chaîne logistique, qui visent les sous-traitants d'une entreprise pour l'atteindre, sont en forte progression. Ce mode d'action est dangereux et exige de l'attaquant un investissement légèrement accru, car la protection initiale est parfois renforcée, mais il permet d'accéder à d'autres structures protégées en visant un maillon faible.

À l'avenir, le monde sera de plus en plus numérisé. Les véhicules connectés, les maisons connectées, les villes intelligentes et la dépendance croissante aux réseaux sociaux renforcent la menace cyber, tant en envergure qu'en profondeur et en technicité. En outre, les auteurs d'attaques sont de plus en plus désinhibés.

La détection des menaces et des tactiques mises en œuvre est globalement placée sous la responsabilité de l'ANSSI. Toutefois, un protocole prévoit qu'elle fasse appel au Comcyber si elle est dépassée ou si elle a besoin de soutien.

Pour ma part, je traite une menace propre aux armées- en ce sens, le Comcyber constitue aussi le bouclier du MINARM- en assurant la défense de 1 800 systèmes différents. Cette diversité – systèmes d'armes, systèmes de communication, systèmes d'information, systèmes industriels – se double d'une grande variété de niveaux de classification, du niveau non protégé jusqu'au très secret-défense. Il faut donc couvrir un large spectre de technicité, d'autant que le souhait des armées est d'aller vers toujours plus de numérisation et d'interopérabilité, pour échanger très rapidement et prendre l'adversaire de vitesse. Chaque interconnexion de réseaux signifie pour moi une part de fragilité supplémentaire sur laquelle veiller.

Les adversaires sont nombreux et dotés de motivations très diverses. S'ils sont un peu moins menaçants pour moi que pour la société civile, un peu moins bien armée structurellement, je n'en ai pas moins affaire à des attaquants de très haut niveau, qui sont soit des cybercriminels, soit des services de renseignement ou encore des hacktivistes, les uns étant souvent liés aux autres. Ces attaquants prennent le temps nécessaire pour développer

leurs attaques, usant de moyens potentiellement gigantesques pour investir les réseaux et trouver le maillon faible.

Les secteurs aérien et naval sont statistiquement les plus touchés par les attaques de la chaîne logistique. Par ailleurs, nous devons travailler à résorber notre vulnérabilité potentielle sur le champ de bataille, où la proximité de nos forces avec l'adversaire fragilise, dans le spectre électromagnétique, l'intégrité de nos systèmes de liaison radio.

Dans les conflits, le cyber est devenu un espace central de conflictualité. Le conflit en Ukraine, que j'ai eu l'occasion d'analyser devant vous sous l'angle cyber, démontre qu'il est possible, avec une bonne défense et en commençant tôt – dès 2014 en l'espèce –, non d'annuler mais de limiter l'impact des attaques. Par ailleurs, ce monde reste un univers très discret, secret et invisible. Ce que l'on dit de l'Ukraine, c'est ce que l'on en sait, mais nous n'en savons pas tout.

J'en viens aux grandes orientations de la réponse apportée par la LPM 2024-2030. Il n'est pas désagréable de me présenter devant vous en disant que j'ai le sentiment, sur ce point, d'avoir été entendu. Ce n'est pas neutre : compte tenu des préoccupations suscitées par le retour de la haute intensité, chaque composante des armées, chaque armée, chaque spécialité a forcément des demandes importantes à faire valoir. Comme je l'ai dit lors de ma précédente audition, c'est un gros édredon d'expression de besoins qu'il faut faire entrer ensemble dans une valise de ressources, non extensibles à l'infini.

Les crédits accordés au cyber sont multipliés par trois. Il s'agit essentiellement d'atteindre l'objectif fixé par la Revue nationale stratégique (RNS) 2022 : « une résilience cyber de premier rang ». Ces financements seront distillés vers les entreprises du domaine Cyber françaises et européennes, notamment dans le cadre de la recherche et développement (R&D). En les faisant monter en gamme, nous obtiendrons des améliorations technologiques qui permettront par la suite de développer des capacités utiles à nos grandes entreprises et à nos PME.

L'effort d'investissement s'articule autour de quatre axes : le chiffre, la lutte informatique défensive (LID), la lutte informatique offensive (LIO) et la lutte informatique d'influence (L2I).

Le chiffre est le socle de notre protection. Nous avions au départ une dette technique élevée en la matière. La précédente LPM a amplement contribué à faire de la réparation, en y consacrant environ 60 % de l'investissement important consenti dans le cyber. L'effort sera poursuivi dans la prochaine LPM. Il faut sans cesse développer nos compétences en la matière, car la technologie évolue et l'adversaire trouvera des moyens pour décrypter nos informations. Le chiffre reçoit donc une part importante de notre budget. Il y va de la sécurisation de nos liaisons de données et de la garantie de notre interopérabilité avec les alliés, qui suppose, pour échanger avec eux des messages importants et confidentiels, d'être crédible et de disposer d'un niveau de chiffrement de haute qualité.

En outre, la forte augmentation de nos crédits permet d'en consacrer une part significative à la LID, à la LIO et à la L2I.

En matière de LID, nous aurons la capacité d'étendre nos moyens de supervision, de détection et de caractérisation. La LID consiste à patrouiller sur les réseaux pour détecter les attaques au plus tôt et intervenir promptement pour les contrer. Il s'agit de vérifier, grâce à des sondes et à des moyens positionnés sur les postes de nos militaires, que nous ne sommes pas attaqués.

Des audits et des homologations permettent de protéger les systèmes en amont. Le jour où nous sommes attaqués, des équipes font des vérifications, remontent à la source du logiciel malveillant, font de l'investigation numérique, tentent d'identifier les attaquants et défendent le plus rapidement possible les systèmes susceptibles d'être contaminés.

Dans ce domaine, nos effectifs seront renforcés. Nous nous appuyons aussi sur la réserve et attendons beaucoup des cinq mesures de simplification dont celle-ci fera l'objet dans le cadre de la LPM 2024-2030. Nous faisons appel, dans le cyber, à la part de la réserve dite de compétence. Nous adressons à nos centres, notamment celui de Rennes, ainsi qu'aux unités cyber des armées, des profils de bon niveau. Nos effectifs devraient augmenter de 300 réservistes actuellement à 500. Nous comptons beaucoup sur les mesures de simplification de la réserve pour que cette augmentation n'immobilise pas trop de personnel pour la rédaction des ordres de mission et l'organisation du suivi.

Sur la LIO, je ne pourrai pas m'étendre très longtemps, en raison du secret qui l'entoure. Dévoiler les capacités dont nous disposons et celles que nous visons demain donne de précieux indices à nos adversaires potentiels. Je me contenterai d'indiquer que nous développons, surtout à l'échelon stratégique, un premier niveau de maturité de qualité.

La L2I est en quelque sorte le petit nouveau de la LPM 2024-2030. Elle ne figurait pas dans la précédente. Cet état de fait illustre la souplesse dont doit faire preuve, selon nous, notre vision du cyber, qui ne sera pas en 2030, ni même en 2027, ce qu'il est en 2023. Nous devons conserver une certaine flexibilité, une capacité d'ajustement pour faire face aux menaces qui émergeront.

La L2I a émergé en France avec la lutte contre Daech, qui recrutait nos jeunes par une propagande agressive et brutale, faite d'incitation à la violence et à la haine. Après des débuts modestes à partir de 2015, elle a connu une amplification majeure dans le cadre de nos affrontements en Afrique avec des acteurs désinhibés travaillant globalement contre la présence française en Afrique et cherchant à nous décrédibiliser.

La L2I consiste à détecter et à caractériser l'adversaire, ce qui n'est pas simple, car il faut distinguer un acteur seul et hostile par nature ou par conviction personnelle, d'une menace construite et structurée, disposant de relais d'amplification importants. Notre travail nous a permis de progresser ; la LPM 2024-2030 doit nous permettre de passer de l'artisanat à l'industrialisation. Dans ce cadre, nous allons doubler les effectifs affectés à la L2I.

J'en viens à notre stratégie de montée en puissance. Lorsque j'ai pris mes fonctions, j'ai tracé trois lignes d'opération.

La première est celle des ressources humaines. Au-delà des moyens financiers, la principale richesse, le cœur même de la Cyberdéfense, ce sont ses ressources humaines. Elles constituent également son principal défi. Pour trouver la ressource dans un pays qui, dans le

domaine de la cybersécurité, produit chaque année moins d'ingénieurs et de techniciens qu'il n'ouvre de postes, nous devons trouver les bons ressorts pour davantage recruter, former et fidéliser. Ce travail s'impose d'autant plus que nous devrons dépasser les 5 000 cybercombattants à l'horizon 2030.

Pour recruter, nous avons des atouts, notamment le sens de la mission – les jeunes cherchent du sens ; chez nous, ils en trouvent – et l'esprit d'équipe, de corps et de camaraderie. Par ailleurs, nous dispensons des formations initiales et continues qui maintiennent le niveau et sont très prisées. La possibilité de progresser dans l'institution existe aussi dans le cyber, qui donne accès à l'escalier social, que nous préférons à l'ascenseur social, car il s'agit de s'élever par l'effort. Le défi technique que représente la diversité des systèmes des armées, qui est unique en son genre, permet à un jeune ayant un bon niveau de compétence technique de progresser continuellement. En outre, nous proposons des missions en opérations extérieures (Opex), dans des milieux particuliers et dans les trois armées.

Nous avons aussi des handicaps, sur lesquels nous travaillons, notamment la fluidité du recrutement, qui pâtit parfois, notamment dans la réserve, de lourdeurs administratives. Nous avons créé un bureau d'appui au recrutement cyber, très présent au Campus Cyber, à Paris, pour faire évoluer les choses. Un jeune qui veut être militaire n'a qu'à pousser la porte d'un centre d'information et de recrutement des forces armées (CIRFA) pour obtenir satisfaction. Un jeune doté de compétences informatiques et de cybersécurité désireux de servir son pays n'a pas toujours ce réflexe, car il voit dans les CIRFA des navires, des soldats sur le terrain et des pilotes de l'armée de l'air, et se dit « Ce n'est pas mon truc » ou « Je n'ai pas la condition physique pour faire cela ». L'idée est d'aller chercher ces profils et de les attirer vers nous, en comptant sur les armées pour les recruter sur leurs droits et sous leurs uniformes.

Les salaires constituent un handicap, ce qui n'a rien d'une surprise s'agissant de la fonction publique. Des travaux sont en cours pour améliorer la situation. S'agissant du télétravail, il reste rare dans nos structures. Nous devons prendre en compte les impératifs de réalisation collective de la mission, de la confidentialité associée et de l'esprit de corps et de camaraderie que j'évoquais précédemment. Le télétravail concerne donc essentiellement des travaux de développement et d'expertise. En revanche, nous réfléchissons à des solutions pour favoriser le travail en région. Dernier handicap : la faible lisibilité initiale des parcours, qui se sont structurés *ad hoc* au sein de l'État. Nous offrons désormais des parcours potentiellement très complets. Un jeune qui s'engage chez nous peut ensuite travailler à l'ANSSI ou à la DGSE, et revenir chez nous ensuite. Des parcours variés et valorisants sont possibles dans le domaine technique.

Plus généralement, en matière de ressources humaines, nous avons conscience que nous ne garderons pas la plupart de ceux que nous recrutons pendant vingt-cinq ou trente ans. Nous nous inscrivons donc dans une dynamique de flux, dont l'armée a certes la culture, mais pour les flux du temps long plus que pour ceux du temps court. Par ailleurs, nous avons le sentiment que nous irriguons la société. La LPM 2024-2030 consent, pour le cyber, un gros effort de formation, dont le budget triple. Nous avons conscience qu'offrir une formation de haut niveau à notre personnel améliore le recrutement, mais s'ils restent moins de cinq ans, nous sommes perdants.

Un projet avec l'École polytechnique visant à développer encore davantage l'excellence nationale en matière de formation initiale, porté par le ministre, est en cours. Divers projets visent à amener les grandes écoles d'ingénieurs vers la cybersécurité. Par ailleurs, le Comcyber a un ancrage fort en Bretagne, où se trouve le pôle d'excellence cyber créé par la région et le ministère. Nous y développons des interactions fortes avec le monde académique, la recherche et les sociétés du domaine cyber.

Ma deuxième ligne d'opération est la recherche de l'excellence opérationnelle portée par l'amélioration de l'intégration des effets cyber aux opérations militaires. En la matière, nous avons développé des capacités de LIO et de L2I de haut niveau ; nous essayons de descendre vers les échelons opératif et tactique, pour mieux appuyer les armées avec les outils et les capacités que nous avons développés. Pour la LID, c'est le contraire : nous partons du bas, les armées disposent déjà de capacités matures et il faut désormais améliorer leur interopérabilité pour consolider l'hypervision qui nous permettra de gagner en efficacité en cas d'attaque majeure Travailler entre domaines de lutte suppose d'établir des priorités, mais la LIO peut appuyer la L2I et la L2I peut appuyer la LID. Ces interactions sont possibles entre les trois domaines de lutte.

Je ne m'étendrai pas sur ma troisième ligne d'opération, les partenariats, faute de temps. À l'échelon national, nous avons un ancrage fort dans la communauté formée par le Centre de coordination des crises cyber (C4), dirigé par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). À l'étranger, nous étendons nos relations partenariales, sous forme bilatérale ou dans le cadre de l'UE.

M. Jean-Michel Jacques, rapporteur sur le projet de loi de programmation militaire 2024-2030. La LPM 2019-2025 a permis de construire et de coordonner les capacités de l'armée en matière de cyber, grâce à la création de 1 500 postes cyber et de la posture permanente cyber.

Comme l'a rappelé le ministre, passer à côté de l'enjeu cyber, c'est passer à côté d'un enjeu majeur. Le budget de 4 milliards d'euros prévu par la LPM 2024-2030 nous permettra de tenir notre rang à l'échelon international. Il faut y ajouter les effets indirects des 8 milliards investis dans le numérique et des 10 milliards de crédits alloués à la recherche et à l'innovation, dans des domaines comme l'intelligence artificielle. Les dispositions de la LPM 2024-2030 permettront-elles à la France de poursuivre le développement d'une cyberdéfense de premier plan face à nos compétiteurs stratégiques ?

Général Aymeric Bonnemaison. Nous suivons de près toute innovation en matière d'intelligence artificielle, d'informatique quantique et dans tout domaine susceptible d'introduire une faille ou une opportunité, selon le côté où l'on se place.

Baisser la garde ou alléger notre effort en matière de cyber, c'est être déclassé. Nous sommes engagés dans une course sans fin. La France est partie relativement tôt, mais pas dans les toutes premières nations. Elle a acquis un niveau d'expertise reconnu grâce à un bon niveau technique et à une approche très opérationnelle du cyber. Si nous relâchons l'effort, nous ne serons plus dans la course.

L'ambition affichée par la LPM 2024-2030 nous permettra de rester en ligne, sous réserve de ce que feront nos compétiteurs. C'est volontairement que j'ai ouvert mon propos

par la menace : beaucoup dépendra de nos compétiteurs majeurs et de notre capacité à nous adapter.

M. Jean-Michel Jacques, rapporteur. J'en déduis que, dans le débat opposant la cohérence et la masse, vous préférez, pour l'investissement dans le cyber, la cohérence ?

Général Aymeric Bonnemaison, commandant de la cyberdéfense. La LPM 2024-2030 fait le choix de la cohérence globale.

S'agissant de l'engagement sur le champ de bataille, l'exercice Orion a montré que le cyber est d'ores et déjà intégré aux manœuvres, comme l'espace d'ailleurs. Peu de pays ont une intégration d'une telle maturité. Nous étudions le retour d'expérience (Retex). Certes, tout n'a pas été parfait, mais l'exercice a permis d'acculturer les armées, en montrant à celui qui sert à bord d'un bâtiment de la marine, dans les forces armées déployées sur le terrain ou dans une base aérienne, l'impact qu'une action cyber peut avoir sur la manœuvre dans son ensemble. Désormais, les officiers chargés d'un commandement ont parfaitement conscience de cette menace.

Mme Sabine Thillaye (Dem). L'ANSSI est pleinement intégrée dans la lutte contre les cyberattaques. La LPM 2024-2030 renforce ses prérogatives, en lui offrant notamment la possibilité de demander le blocage d'un nom de domaine susceptible de porter atteinte à la sécurité nationale et celle de détecter plus facilement les serveurs utilisés par les cyberattaquants. Le Comcyber est en lien avec la Direction générale de la sécurité extérieure (DGSE), la Direction du renseignement militaire (DRM) et la Direction du renseignement et de la sécurité de la défense (DRSD), ainsi qu'avec l'ANSSI pour la LID.

À l'avenir, dans un contexte de forte évolution des menaces cyber, qu'attendez-vous de l'ANSSI en matière de LID ? Les évolutions législatives prévues par la LPM 2024-2030 vous semblent-elles à la hauteur des enjeux actuels et à venir ? Le renforcement de notre arsenal législatif correspond-il à celui effectué par nos partenaires ?

Général Aymeric Bonnemaison. Certains de nos partenaires sont dotés d'un corpus législatif intéressant. Je ne souhaite pas évoquer ce sujet à la place de l'ANSSI, mais je peux souligner que ces évolutions vont dans le bon sens. Tout ce qui nous permettra d'être plus réactifs, et surtout moins naïfs, s'agissant des attaques auxquelles nous pouvons être confrontés, va dans le bon sens.

En matière de défense, du point de vue fonctionnel, je dépends de l'ANSSI, qui me délègue la responsabilité de mes réseaux. L'interaction entre nous est permanente. En matière d'expertise, nous nous aidons mutuellement. À mes yeux, la dynamique générale des évolutions législatives est très favorable.

Mme Anne Genetet (RE). Quels sont les points de vigilance que vous souhaitez porter à notre attention s'agissant des besoins que vous pourriez avoir au cours des sept ans que couvre la LPM 2024-2030 ? Sept ans, c'est long, surtout en matière de cyberdéfense.

S'agissant du recrutement, la LPM 2024-2030 prévoit de développer le recours à l'apprentissage et à la réserve. Comment envisagez-vous de répondre aux enjeux de fidélisation et de recrutement ?

Général Aymeric Bonnemaison. Ma seule demande, pour l'heure, est que nous tenions les 4 milliards ! Surtout, il faudra faire preuve de flexibilité dans leur orientation, en fonction de la menace et de son évolution. De même que nous avons développé la L2I en actualisant la précédente LPM, nous devrons sans doute actualiser la LPM 2024-2030 dans un domaine pour lequel sept ans, c'est très long.

Sur l'apprentissage, le Comcyber compte une trentaine d'apprentis dans ses effectifs. Nous essaierons de développer cette voie de recrutement, notamment grâce aux dispositions relatives à l'apprentissage militaire de la LPM 2024-2030.

Sur la réserve, je n'ai pas les mêmes problèmes que pour la population d'active. De nombreuses entreprises de services du numérique (ESN) me contactent – les aspects déontologiques de la démarche restent à explorer – non seulement pour rester connectées, mais aussi pour fidéliser leurs jeunes, dont la soif de sens peut être étanchée par une présence parmi nous de trois ou quatre semaines par an. Les entreprises elles-mêmes accompagnent le mouvement et me proposent des jeunes qui veulent rejoindre la cyberdéfense, ce qui a été un peu une surprise pour moi.

Par ailleurs, nous communiquons beaucoup. Je n'ai donc aucune inquiétude sur la réserve et le volontariat. Je me préoccupe surtout de la structurer et de l'adosser aux armées à l'échelle régionale. Je suis très concentré sur cet objectif, d'autant que les unités cyber des armées seront plus étroitement liées au Comcyber d'ici la fin de l'année. Il y aura des unités cyber en région, par exemple à Toulon pour la marine et à Mont-de-Marsan pour l'armée de l'air, ce qui nous permettra d'assurer une présence un peu plus territorialisée.

M. Pierrick Berteloot (RN). Chacun comprend que notre armée doit être en mesure de protéger efficacement notre territoire face aux menaces de cyberattaques, et de riposter lorsque cela est nécessaire. La guerre en Ukraine nous a donné l'exemple d'un emploi massif de l'arme cyber dans un conflit de haute intensité sur des cibles variées, et parfois inattendues.

Ainsi, l'attaque par les Ukrainiens de la plateforme comptable de distribution d'alcool russe Egais, début mai 2022, pourrait être à l'origine d'une perte de 28 millions de dollars de droits d'accises pour la Russie, soit l'équivalent de quatorze chars T-80 – exemple concret et édifiant ! En mai également, le satellite européen KA-SAT a fait l'objet d'une attaque, dont la Russie a été accusée. En Afrique, une guerre d'influence est à l'œuvre, qui menace directement nos intérêts, comme l'a montré l'affaire du faux massacre de Gossi, au Mali, monté de toutes pièces par le groupe Wagner pour accuser les forces françaises.

Face à ces risques, la France, qui entend conserver un modèle d'armée complet, doit pleinement s'investir dans le cyber. Telle est la raison de la création du Comcyber il y a cinq ans. Nous avons intégré la cybersécurité dans le concept de sécurité nationale, avec l'ambition de développer une résilience cyber efficace. Cela nécessite des ressources technologiques avancées et des profils aux compétences techniques élevées, à recruter et à fidéliser. Si le domaine militaire cyber est plutôt attractif, il est fortement concurrencé par le secteur privé, plus généreux en matière de rémunérations. Hier, le DGSE a évoqué cet enjeu devant nous.

Parvenons-nous à recruter et à fidéliser les ressources humaines indispensables à la mise en œuvre d'une stratégie de cyber défense nationale ? Avons-nous des moyens matériels et techniques à la hauteur de nos ambitions ?

Général Aymeric Bonnemaison. Sur le recrutement, il faut encore assouplir nos façons de faire, mais nous y parviendrons. L'enjeu, c'est la fidélisation qui, sans atteindre des durées excessives, nous permettra d'avancer.

Dans ce cadre, il faut construire des parcours dans le public, mêlant des expériences chez nous avec d'autres à la DGSE ou à l'ANSSI par exemple. Ces parcours croisés sont d'une très grande richesse. Le cyber présente la singularité, au sein de l'État, de s'être construit autour de gens ayant travaillé dans ces diverses entités et ayant déjà un riche parcours. La qualité des échanges au sein du C4 l'illustrent. Ce qui nous unit est d'être dans la matière depuis plus de dix ans et de nous connaître, donc d'être préoccupés par les solutions que nous devons trouver ensemble.

La fidélisation et plus généralement les ressources humaines sont au cœur de nos enjeux. Notre fragilité tient beaucoup aux salaires, qui sont parfois deux à trois fois inférieurs à ceux offerts par le privé.

M. Emmanuel Fernandes (LFI-NUPES). La sécurité des installations nucléaires civiles et militaires est un sujet fondamental pour notre cyberdéfense. Dans ce domaine, il existe des antécédents, dont nous avons sans nul doute tiré des enseignements.

En 2014, la société *Korea Hydro & Nuclear Power*, qui gère un parc de centrales nucléaires en Corée du Sud, a été cyberattaquée. Des données de la firme ont été volées. En 2010, le virus Stuxnet, conçu par la NSA et par l'unité israélienne 8200, a sévèrement perturbé le programme nucléaire iranien, détruisant plusieurs centaines de centrifugeuses de la centrale de Natanz. Ce sont deux exemples de cyberattaques contre des installations nucléaires civiles ou reliées à un programme militaire. Comment le Comcyber tient-il en compte de la cybersécurité du commandement, du contrôle et des communications nucléaires (NC3) ?

Les moyens financiers supplémentaires prévus par la LPM 2024-2030 pour le domaine du cyber, à hauteur de 4 milliards d'euros sur sept ans, vous semblent-ils de nature à répondre complètement à la criticité des enjeux et à la course de vitesse imposée par la sophistication toujours plus grande des attaques cyber ?

Le rapport annexé évoque l'objectif de renforcer les domaines du renseignement, de la cyberdéfense et du numérique. Toutefois, la cible de ressources humaines n'est pas détaillée à l'horizon 2030. Êtes-vous en mesure de donner des précisions sur les besoins en effectifs et la trajectoire envisagée du progrès en nombre de militaires dédiés à la cyberdéfense ? Vous avez dit espérer plus de 5 000 femmes et hommes, et bien au-delà. Avez-vous des détails à ce sujet ?

Général Aymeric Bonnemaison. J'ai évoqué le haut niveau de protection de nos systèmes et l'effort particulier fait dans le domaine du chiffre. Les exemples de Stuxnet et de la *Korea Hydro & Nuclear Power* sont bien identifiés et travaillés, dans le cadre d'une veille permanente. Nous sommes d'une vigilance extrême à ce sujet. Dans ce domaine, nous

n’avons pas besoin de sensibiliser grand monde, car la notion de secret et les procédures de protection y sont bien établies.

En matière de ressources humaines, je ne peux pas vous donner de chiffres, au risque de vous décevoir. J’ai besoin d’effectifs importants, je me suis exprimé à ce sujet, mais je dois être réaliste : je dois pouvoir recruter et former dans les délais les effectifs que je demande. Il faut donc adopter une pente de croissance réaliste compte tenu de ce que je dois honorer. À ce jour, tous mes droits ne sont pas honorés. Ce que je puis dire, c’est que nous doublerons les effectifs affectés à la L2I et que nous augmenterons significativement ceux affectés à la LID et à la LIO.

Mme Mélanie Thomin (SOC). Vous avez évoqué le pôle d’excellence cyber, issu d’un partenariat conclu entre le ministère des armées et le conseil régional de Bretagne. Enseignante en série technologique, je ne peux qu’abonder dans le sens de ce projet. Votre filière incarne un véritable espoir pour nos jeunes et suscite leur intérêt.

Le cyber fait l’objet d’un effort budgétaire important dans la LPM 2024-2030, à hauteur de 4 milliards. Il s’inscrit dans la continuité de la création du Comcyber en 2017. Le projet de loi confirme la posture permanente cyber des armées et la poursuite des efforts de recrutement. Pouvez-vous nous indiquer si l’effort portera principalement sur le recrutement ou sur le développement et l’acquisition d’outils, voire le MCO ?

Le cyber est souvent associé à l’innovation. Or la recherche d’innovations suppose une capacité d’intégration et des arbitrages entre acquisition et développement interne. Plus généralement, la liberté d’action dans le cyber nécessite surtout une réactivité et une stratégie de surveillance propre, lorsque le Comcyber n’est pas en appui d’une manœuvre interarmes. Comment cette posture est-elle maintenue ? Comment sont assurés les entraînements et leur mise à jour pour la conduite de cette palette de missions très vaste ?

Enfin, dans quelle mesure le développement de la L2I impose-t-il une rupture capacitaire et doctrinale ? Comment la LPM 2024-2030 peut-elle y répondre ?

Général Aymeric Bonnemaison, commandant de la cyberdéfense. S’agissant de nos relations avec l’enseignement secondaire, nous avons lancé un projet de *capture the flag*, pour l’instant circonscrit à l’Île-de-France, mais que nous voulons étendre au-delà, intitulé « Passe ton hack d’abord ». Je l’ai proposé au directeur général de l’enseignement scolaire (Dgesco), qui s’est immédiatement montré enthousiaste. Nous avons mis le projet à l’étude, en fixant un plafond à 1 000 lycéens. Ayant commencé assez tard, au mois de novembre, nous en espérions 300 ; nous en sommes à plus de 900.

Par ailleurs, toutes les formations de spécialité cyber dans les écoles ne sont pas armées, notamment parce que nous manquons de jeunes femmes, qui s’autocensurent dans le numérique. Le Dgesco et moi-même avons donc encouragé les lycéennes à participer au projet ; nous en avons aujourd’hui plus de 200.

L’idée est de montrer, sous une forme ludique, que le cyber n’est pas uniquement un monde réservé aux meilleurs mathématiciens, et qu’il est attrayant et accessible à tous. Ce programme marche très bien ; les professeurs encadrent bien les jeunes avec l’appui de nos réservistes. La remise des prix aura lieu le 10 mai au Campus Cyber.

Notre effort porte sur tous les fronts, du recrutement au MCO en passant par la formation et le développement d'outils spécifiques. Aucun n'a la priorité. Nous ne sommes jamais à l'arrêt : la lutte informatique, c'est chaque jour, week-ends compris. La veille, la vérification des systèmes et la caractérisation des attaques sont quasi-permanentes. Nous sommes dans le monde réel.

Dans les autres métiers, les gens s'entraînent en vue de leur déploiement en opération. Dans le cyberespace, le triptyque compétition-contestation-affrontement est quasi-permanent. Notre travail d'innovation est itératif mené avec la DGA et certains industriels. Nous testons des solutions de façon assez souple ; si elles sont performantes, nous entrons dans un cycle de programmation pour les acquérir et maintenir leurs capacités. La proximité avec la technologie est dans l'ADN du Comcyber.

Mme Anne Le Hénanff (HOR). Deux de nos collègues ont rédigé un rapport d'information sur le bilan de la LPM 2019-2025. Il formule plusieurs recommandations, notamment celle de développer davantage les partenariats à l'échelle nationale, avec les services de l'État chargés du domaine cyber, notamment l'ANSSI, les services de renseignements, la DGA et le ministère de l'Europe et des affaires étrangères, ainsi qu'aux échelles européenne et internationale. Compte tenu des crédits et des orientations du projet de loi de programmation militaire que nous examinerons bientôt dans l'hémicycle, je souhaite savoir comment le Comcyber envisage de renforcer ses partenariats, avec qui, selon quelles modalités, en s'inscrivant dans quelle stratégie et avec quels objectifs.

Général Aymeric Bonnemaison. C'est l'une des leçons de l'Ukraine : lorsque l'on est attaqué, l'échange de données techniques est essentiel.

Nous avons d'ores et déjà noué des partenariats bilatéraux avec plusieurs pays, avec lesquels une confiance certaine s'est instaurée. Le seul bémol aujourd'hui est que ma ressource pour en assurer le suivi est comptée.

J'ai poursuivi la démarche initiée par mon prédécesseur dans le cadre de la présidence française du Conseil de l'Union européenne (PFUE), consistant à réunir les commandants cyber européens. La première édition a été un peu perturbée par le covid, pas la deuxième. La troisième a eu lieu il y a quinze jours à Bruxelles, dans les locaux de l'Agence européenne de défense (AED), avec un certain succès : dix-neuf pays étaient représentés. À notre grande satisfaction, les Comcyber espagnol et belge organiseront les deux prochaines réunions, lorsque leurs pays respectifs assureront la présidence du Conseil de l'UE. Cette démarche, initiée et portée à bout de bras par la France, se poursuit donc. Nous y développons un vrai niveau de confiance, ce qui est essentiel.

Pour cette dernière séquence, nous avons entendu deux témoignages sur la réserve, celui des Estoniens et celui des Suisses, qui sont les plus avancés à ce sujet, grâce à la conscription. Ils ont développé une approche intéressante, permettant notamment de déterminer comment sélectionner les profils, comment les faire revenir et comment poursuivre la coopération. Leurs témoignages, mettant en lumière les différences d'approche culturelle, ont donné lieu à de riches débats.

Nous avons également abordé le sujet de la solidarité stratégique et de la façon de s'entraider. Jusqu'à présent, chaque pays, et la France la première, souscrivait à l'idée qu'il devait commencer par développer ses propres capacités et atteindre un premier niveau de maturité. Le conflit en Ukraine nous a fait évoluer. Désormais, nous proposons aux nations en difficulté, sous réserve de disposer d'une équipe, de leur porter assistance ou de les conseiller. D'autres projets d'entraide, par des équipes mixtes (ie internationales), sont proposés par des partenaires. Nous construisons cette solidarité pas à pas.

Le troisième sujet que nous avons abordé est le partage d'informations. De nombreux services cyber émanent de structures de renseignements, où l'échange a davantage lieu en bilatéral qu'en collectif. Ils doivent passer d'une culture du *need to know* à une culture du *need to share*. Dans la LID, le partage d'informations est une nécessité.

Cela suppose de mettre au point des systèmes permettant de communiquer et d'échanger rapidement. Nous devons encore définir le type d'information que nous pouvons échanger, ce qui comporte des aspects techniques. L'essentiel est que, si un pays est attaqué et détecte le logiciel malveillant qui l'a attaqué, il nous le transmette rapidement pour nous permettre de l'intercepter. Plus l'échange sera rapide, plus notre défense collective sera performante.

S'agissant de l'OTAN, des projets sont en cours. Nous voulons éviter les doublons avec ceux que nous lançons dans le cadre de l'UE. Nous verrons comment coordonner l'ensemble. Quoi qu'il en soit, un premier niveau de confiance entre Comcyber est instauré, même si leurs périmètres respectifs diffèrent sensiblement.

M. le président Thomas Gassilloud. Je suppose que, lorsqu'un pays attaqué vous signale un logiciel malveillant, vous transmettez son signalement au sein du C4 ?

Général Aymeric Bonnemaison. Bien sûr.

Mme Delphine Lingemann (Dem). Depuis le début de la guerre en Ukraine, les cyberattaques se sont développées de façon exponentielle. Elles ont augmenté de 140 % en 2022.

Face à ces risques, la mutualisation à l'échelon européen est devenue cruciale. En renfort du *Cyber Resilience Act* européen annoncé en septembre dernier, visant à intégrer des dispositifs de protection aux objets connectés dès leur phase de conception, un *Cyber Solidarity Act* sera présenté dans les prochains jours. Il a l'ambition de mettre en œuvre un bouclier cyber européen. Dix-sept États membres, dont la France, se sont d'ores et déjà positionnés sur cette proposition de règlement.

Tout cela suppose de partager des ressources humaines et des moyens financiers. Un investissement de plus de 1 milliard d'euros est prévu, financé aux deux tiers par l'Europe, pour la construction de cinq ou six centres opérationnels de sécurité et la création d'une académie européenne des compétences en matière de cybersécurité. Le Fonds européen de défense (FED) permettra d'accompagner le financement de ces nouvelles structures, dont la LPM 2024-2030 tient compte pour permettre à nos armées de s'adosser à ces deux projets européens. La France se positionnera-t-elle pour accueillir un centre opérationnel de sécurité ?

Par ailleurs, je puis vous dire, en tant qu'enseignante dans une école d'ingénieurs, que l'industrie de défense est toujours absente de certaines écoles d'ingénieurs.

M. Frédéric Boccaletti (RN). La revue stratégique de cyberdéfense, publiée en 2018, jette les bases d'une ambitieuse stratégie cyber pour les armées. Rappelés à plusieurs reprises dans le rapport annexé à la LPM 2024-2030, les enjeux cyber doivent impérativement être pris en compte dans la conduite des opérations militaires. La supériorité militaire de demain résidera dans la maîtrise et la combinaison du matériel – l'opérationnel militaire classique – et de l'immatériel – l'offensive informatique. Nos corps d'armée sont-ils suffisamment sensibilisés aux enjeux de cyberdéfense pour envisager une coopération interarmées ?

M. Christophe Blanchet (Dem). Dans le rapport d'information sur les réserves que Jean-François Parigi et moi-même avons rédigé, nous évoquons, aux côtés de la réserve opérationnelle que vous avez évoquée, la réserve citoyenne, qui remplit des missions de sensibilisation aux risques cyber, d'aide au recrutement d'experts cyber et de rayonnement au sein des écosystèmes cyber industriels et académiques. En 2019, vous aviez 500 réservistes citoyen et deviez atteindre l'objectif de 4 000. J'aimerais savoir où vous en êtes et quel objectif vous visez dans le cadre de la LPM 2024-2030.

Vous avez évoqué le recrutement de volontaires auprès des entreprises. Comme nous l'avait indiqué votre prédécesseur, il ne serait pas admissible qu'ils s'engagent dans un but mercantile de promotion de leur entreprise. Prévoyez-vous de poser des jalons de précaution ? Quels sont vos systèmes de vigilance à ce sujet ?

Nos échanges dans le cadre du groupe de travail territoire national ont démontré que les critères d'aptitude médicale doivent être adaptés s'agissant du cyber. Une personne en fauteuil roulant peut-être un excellent cyber-combattant sans avoir toutes les aptitudes militaires. La LPM 2024-2030 prévoit-elle une telle levée de dispositions pour accompagner votre commande ?

Vous avez évoqué le cas de jeunes techniquement compétents mais hésitant à pousser la porte d'un CIRFA. La solution au problème ne réside-t-elle pas dans un lieu unique, qui s'appelle « Garde nationale », où recruter puis diriger les gens ?

Général Aymeric Bonnemaison. Le bouclier cyber promu par la Commission européenne relève d'une dynamique intéressant davantage l'ANSSI. Nous étudierons la façon de nous adosser aux structures prévues, notamment en matière de formation. Sans préjudice de ce que vous en dira le directeur général de l'ANSSI, je considère que tout ce qui contribue à une protection collective européenne va dans le bon sens. Il en résulte une véritable prise de conscience des enjeux en Europe. Dans le cas présent, il restera à déterminer comment mettre en œuvre concrètement ce projet mais nous partageons l'ambition affichée.

Sur la réserve citoyenne, je fais mon mea culpa : nous ne sommes pas bons. Nos effectifs ont sensiblement diminué depuis 2019 parce que nous avons privilégié la réserve opérationnelle. J'en ai dressé un premier bilan et nous allons la reconstruire.

S'agissant des ESN, nous réfléchissons à des protocoles visant à éviter qu'elles ne débauchent chez nous plus que de raison. Le dialogue est bon et franc jusqu'à présent. Le

message est bien passé auprès des sociétés concernées. Je suis optimiste ; nous arriverons à construire intelligemment des parcours avec les entreprises françaises.

Sur l'adaptation des critères d'aptitude, nous avançons pas à pas. J'essaie de faire bouger les lignes, y compris pour les réservistes. Nous poursuivons nos efforts en lien avec la DRHMD et la SSA.

S'agissant de la coopération interarmées, nous y travaillons beaucoup. Le chef d'état-major des armées (Cema) a donné une forte impulsion pour la prise en compte de la fonction stratégique d'influence, de l'hybridité et des nouveaux domaines de lutte en général. L'impulsion vient d'en haut. Nous avons donné un gros coup d'accélérateur à l'automne, en prévision de l'exercice Orion, pour intégrer l'espace, la lutte informationnelle et le cyber dans la manœuvre interarmées.

Par ailleurs, la transformation à venir du Comcyber, visant notamment à améliorer l'identification des unités cyber des armées qui interagiront avec nous et qui seront potentiellement sous notre contrôle opérationnel, améliorera la fluidité entre le Comcyber et les armées. Les trois chefs d'état-major d'armée sont favorables à cette convergence.

S'agissant de la Garde nationale et de son rôle dans le développement du service national universel (SNU), nous avons mené une expérimentation dans le Sud-Ouest lors de Journées de la Défense et du Citoyen, qui a montré une très forte adhésion des jeunes. Ce format est prometteur : il permet à des jeunes ayant abandonné trop tôt l'étude des sciences d'y revenir, avec une vision plus ludique que l'approche un peu austère qui prévaut en France. De nombreux jeunes devraient être intéressés, d'autant qu'ils pourront y trouver de réels débouchés professionnels.

M. le président Thomas Gassilloud. Mon général, je vous remercie d'avoir répondu à nos questions.

*

* *

La séance est levée à douze heures.

*

* *

Membres présents ou excusés

Présents. - M. Pierrick Berteloot, M. Christophe Blanchet, M. Frédéric Boccaletti, M. Vincent Bru, M. Emmanuel Fernandes, M. Jean-Marie Fiévet, M. Thomas Gassilloud, Mme Anne Genetet, M. Jean-Michel Jacques, M. Loïc Kervran, M. Jean-Charles Larsonneur, Mme Anne Le Hénanff, Mme Delphine Lingemann, Mme Josy Poueyto, Mme Sabine Thillaye, Mme Mélanie Thomin

Excusés. - M. Xavier Batut, M. Julien Bayou, M. Mounir Belhamiti, M. Christophe Bex, Mme Yaël Braun-Pivet, M. Steve Chailloux, Mme Cyrielle Chatelain, M. Yannick Favennec-Bécot, M. Bastien Lachaud, M. Olivier Marleix, M. Pierre Morel-À-L'Huissier, Mme Valérie Rabault, M. Fabien Roussel, Mme Isabelle Santiago, M. Mikaele Seo, Mme Nathalie Serre