ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
10 juin 2026
Séance de 11 heures

Compte rendu n° 75

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

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

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures.

M. le président Jean-Michel Jacques. Mes chers collègues, dans le cadre de notre cycle « Guerre hybride et continuum de conflictualités », nous avons le plaisir de recevoir le général de division aérienne Emmanuel Naëgelen, commandant de la cyberdéfense au ministère des armées depuis 2025. Mon général, vous avez par ailleurs été de 2021 à 2025 directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Nous recevons également le général de division Patrick Touak, chef du commandement du ministère de l'Intérieur dans le cyberespace depuis janvier 2026.

Le cyberespace est devenu un théâtre d'affrontements permanents. Cet univers voit notamment l'émergence et la croissance de réseaux de criminalité, dont certains présentent une porosité avec des puissances étrangères, notamment la Russie et la Corée du Nord. Ces agresseurs déploient des stratégies qui visent nos entreprises, nos administrations, nos institutions civiles ou militaires, afin d'essayer de nous déstabiliser, voire parfois de nous rançonner.

Les armées disposent d'une organisation cyber robuste. Le commandement de la cyberdéfense, le Comcyber, est responsable des opérations pour le domaine cyber et de la protection des systèmes d'information de l'état-major des armées. La création en 2025 du commissariat au numérique de défense est venue parachever le dispositif de résilience informatique du ministère des armées.

Le rôle du commandement du ministère de l'Intérieur dans le cyber, moins connu de notre commission, s'inscrit dans l'action de la police judiciaire et dans la lutte contre la cybercriminalité, qui constitue l'une des dimensions de la guerre hybride. Nous serons à ce titre particulièrement attentifs à vos propos, général.

Face à la complexité des techniques, des logiciels et à la densité croissante des cyberattaques, l'action doit être interministérielle. Votre présence à tous les deux aujourd'hui témoigne de ce *continuum* de sécurité et de défense. Il nous semblait en effet pertinent de vous recevoir, messieurs les généraux, afin que vous évoquiez cette stratégie de cyber défense. Sans plus tarder, je vous cède la parole.

M. le général de division aérienne Emmanuel Naëgelen, commandant de la cyberdéfense au ministère des armées. Je vous remercie pour cette invitation dans le cadre de votre cycle relatif à la guerre hybride. Elle me permettra d'évoquer, du point de vue des armées, le sujet des menaces cyber, qui constituent une illustration parfaite de ce caractère hybride et montrent la nature des rapports de puissance auxquels nous devons faire face aujourd'hui.

Face à des attaques dans le cyberespace qui ciblent déjà les armées françaises, pouvoir se défendre relève de la nécessité la plus absolue si nous voulons gagner le combat dans cet espace, mais aussi dans les autres milieux, les milieux plus classiques. Gagner ce combat dans le cyberespace est en effet vital, d'autant plus que ses impacts sont extrêmement vastes. Cette lutte est souvent invisible, mais elle rejaillit dans le monde réel et engendre un impact direct sur nos capacités opérationnelles à commander et à agir, sur terre, en mer, dans le ciel et aujourd'hui dans l'espace.

Pour illustrer ce message, j'articulerai mon propos en trois parties : la description de cette menace cyber telle que nous l'observons dans les armées ; les efforts menés en propre et avec nos partenaires de l'équipe France de la cybersécurité ; et enfin, l'impératif de se préparer au combat de demain, celui de la haute intensité. À ce titre, nous serons probablement confrontés aux technologies de rupture telles que l'IA et l'ordinateur quantique.

En premier lieu, la société dans son ensemble s'est numérisée dans tous les domaines et les armées n'échappent évidemment pas à cette évolution. Cette numérisation nécessaire les expose toutefois à des risques particuliers. Le directeur général de l'Anssi, Vincent Strubel, a dû vous indiquer que la menace cyber, et donc les attaques informatiques, évoluent constamment, malheureusement dans un seul sens. Cette menace n'a cessé de croître, à la fois en volume et en sophistication. Du point de vue des armées, les attaques cyber font peser une menace sur trois cercles concentriques ou presque concentriques.

Le premier cercle, assez extérieur aux armées, mais néanmoins capital, concerne les infrastructures critiques. On ne pourrait pas mener un conflit de haute intensité sans hôpitaux, sans électricité, sans opérateurs de télécommunications ou opérateurs de transport. Or, ces infrastructures critiques sont de plus en plus souvent visées par des cyberattaquants, en temps de paix comme en temps de guerre, comme l'ont démontré les attaques en Ukraine depuis 2014 ou plus récemment les attaques en Pologne fin 2025. Si ces attaques informatiques contre des infrastructures critiques visent *a priori* à déstabiliser des États, elles peuvent évidemment venir aussi perturber les opérations militaires.

Le deuxième cercle concerne nos fournisseurs. On ne peut pas faire la guerre sans approvisionnement en armement, en munitions, mais aussi en nourriture ou en matériel divers. Les chaînes d'approvisionnement des armées sont ainsi de plus en plus ciblées, à des fins d'espionnage quand il s'agit d'équipements de haute technologie, mais aussi à des fins de sabotage, quand il s'agit de biens beaucoup plus communs, classiques.

Le troisième cercle est le cercle le plus intérieur, le cœur de nos intérêts, celui des armées françaises elles-mêmes, qui constituent directement une cible stratégique de premier plan. Deux principales raisons y concourent : les données classifiées que nous détenons, mais aussi notre rôle dans la défense de la nation. Les attaques contre le ministère des armées menées par nos compétiteurs stratégiques cherchent donc à compromettre très directement des secrets de la défense nationale. En cas de conflit, elles viseraient certainement aussi à nous empêcher de nous servir de nos systèmes de commandement, de nos armements, au moment le plus critique.

Je vous parle ici d'attaques très sophistiquées, généralement menées par des services de renseignements adverses. Mais nous observons aussi de plus en plus des attaques moins pointues sur le plan technique, comme des faux sites web. Ces dernières visent ainsi à discréditer nos armées et à créer une perte de confiance des citoyens envers leurs institutions.

Ces trois cercles ne sont pas véritablement concentriques, tant les systèmes d'information des armées et du ministère sont interconnectés avec leur écosystème. Quoi qu'il en soit, ces menaces sont d'autant plus préoccupantes qu'elles émanent d'acteurs très variés, dont certains sont évidemment soutenus par des États rivaux.

Généralement, cette menace est classée en trois catégories : les criminels ou cybercriminels ; les États et leurs services de renseignement ; et les « hacktivistes », c'est-à-dire des partisans. Cependant, ces catégories ne sont pas complètement étanches, et même de plus en plus poreuses. À titre d'exemple, des hacktivistes de la Cyber Army of Russia revendiquent très clairement leur alignement sur le pouvoir russe.

Cette porosité entre ces groupes rend évidemment beaucoup plus difficile l'identification des commanditaires et de leurs intentions. En outre, il existe également des acteurs privés, des entreprises qui développent des services d'attaque informatique. Ces derniers sont généralement présentés comme des moyens de lutte contre le terrorisme ou la grande criminalité, mais bien souvent, les officines qui les emploient sont dédiées à des finalités bien moins légitimes ou licites, comme l'espionnage industriel ou scientifique.

Les armées françaises évoluent dans cet environnement très agressif, au sein duquel elles constituent une cible bien défendue, mais de choix. Nous sommes dès à présent visés régulièrement par des attaques informatiques, issues notamment d'acteurs russes. Les armées sont aussi victimes d'attaques informationnelles, évidemment non revendiquées, même si elles laissent peu de doute sur leurs commanditaires.

À titre d'exemple, le 15 mars 2024 un site frauduleux qui s'appelait « s'engager-ukraine.fr » et reprenait la charte graphique de l'armée de Terre, annonçait le recrutement de 200 000 soldats à des salaires d'environ 5000 euros pour combattre en Ukraine. Rapidement dénoncé par le ministère des armées, le site a pu être fermé quatre heures après sa mise en ligne, notamment grâce à l'aide de Viginum.

Ce genre d'exemple illustre le fait que le cyberespace est en réalité aujourd'hui un miroir grossissant des tensions géopolitiques existant dans le monde physique. En effet, les rapports de force s'expriment dans le cyberespace comme dans les autres milieux classiques, mais souvent de manière beaucoup plus désinhibée, aujourd'hui. À ce titre, l'attaque subie par la Pologne le 29 décembre 2025, qui aurait pu entraîner un blackout électrique, représente une parfaite illustration de cet effet miroir grossissant. Manifestement, bien que la Pologne soit en paix aujourd'hui, elle a subi une attaque coordonnée massive, qui ne présentait aucun intérêt en termes d'espionnage, mais dont les conséquences auraient pu être catastrophiques pour les citoyens polonais.

Cette situation n'est pas nouvelle pour les armées, qui ont établi dès les années 2010 le constat de l'emploi du cyberespace dans le cadre d'une conflictualité masquée, sous le seuil. C'est la raison pour laquelle un Comcyber a été créé en 2017, pour rassembler dans un commandement opérationnel unique l'ensemble des forces de cyberdéfense des armées. Il revient ainsi au Comcyber de concevoir, planifier et conduire les opérations militaires dans le cyberespace.

Ces opérations militaires sont en réalité de trois types et reflètent trois finalités. La première finalité ou « finalité primordiale » concerne la lutte informatique défensive (LID). Il s'agit en fait de défendre nos systèmes et nos réseaux, passant par la détection et la caractérisation des attaques, mais aussi la capacité à déployer des groupes d'intervention pour les faire cesser.

Le deuxième type de lutte est relatif à la lutte informatique d'influence (L2I). Il s'agit de détecter les attaques informationnelles qui visent les armées. Nous le faisons depuis un certain temps, notamment depuis la lutte contre la propagande de Daech. Par ailleurs, nous avons évidemment fait face aux opérations de désinformation russes en Afrique jusqu'à l'année dernière. Désormais, nous sommes une des nations les plus avancées dans la L2I. Naturellement, nous n'agissons pas seuls et intervenons fréquemment avec Viginum.

Enfin, le dernier type de lutte est relatif à la lutte informatique offensive (LIO). La LIO consiste ainsi à mener des attaques informatiques pour obtenir du renseignement sur nos adversaires ou neutraliser des systèmes informatiques de commandement, par exemple. Cette capacité est très stratégique pour les armées, et surtout d'une très grande sensibilité pour préserver nos moyens d'action.

Nous ne menons pas seuls ce combat, mais en compagnie du Comcyber du ministère de l'intérieur (Comcyber-MI), dès lors qu'il s'agit de cybercriminalité, mais également de l'Anssi. L'Anssi, en sa qualité d'autorité nationale, est chargée d'aider les victimes de cyberattaques. Mais en cas de crise majeure, si les capacités de l'Anssi devaient se révéler insuffisantes ou indisponibles, il est prévu que mon commandement puisse venir en appui de l'Agence. Ce type de scénario a été instruit lors des Jeux olympiques de Paris 2024 et nous le réitérerons d'ailleurs pour le G7 à Évian, la semaine prochaine. Nos relations avec Viginum sont extrêmement fluides, afin de partager des savoir-faire, des méthodes, des techniques et notre perception de la menace.

Enfin, nous menons un travail au niveau interministériel et sommes notamment intégrés dans deux structures de coordination interministérielle. Il s'agit d'une part du C4, le centre de coordination des crises cyber qui réunit autour du secrétariat général de la défense et de la sécurité nationale (SGDSN) les entités publiques compétentes en matière de cyber : le Comcyber, l'Anssi, la direction générale de l'armement (DGA), le ministère de l'Europe et des affaires étrangères, la direction générale de la sécurité intérieure (DGSI) et la direction générale de la sécurité extérieure (DGSE). Ce C4 est très utile, car il nous permet de caractériser la menace, mais aussi de proposer des options de réponse à nos autorités.

L'autre enceinte interministérielle est constituée par le comité opérationnel de lutte contre les manipulations de l'information (Colmi). Inspiré par le modèle du C4 et également organisé autour du SGDSN, le Colmi permet de réunir les acteurs du ministère des armées, du ministère de l'intérieur, du ministère de l'Europe et des affaires étrangères, et Viginum. Pour nous, il est essentiel de participer à ces structures de coordination, qui permettent d'apporter un ensemble de réponses cohérentes aux menaces hybrides qui touchent le ministère et les armées.

Enfin, dans le domaine cyber, rien n'est jamais acquis. Il nous faut sans cesse poursuivre nos adaptations, pour être en mesure d'anticiper autant que possible les menaces de demain. Ainsi, dès aujourd'hui, en cohérence avec la vision du chef d'état-major des armées, nous nous préparons aux chocs en vue d'un possible choc de haute intensité d'ici à trois à quatre ans. Un tel choc serait certainement annoncé ou précédé par des attaques massives dans le cyberespace.

C'est la raison pour laquelle notre priorité consiste, encore une fois, à renforcer nos défenses. Ce renfort est essentiel si nous voulons conserver notre liberté de manœuvre et la performance opérationnelle de nos armées. Cette mission, prioritaire pour nous, est également

très exigeante. Il est de coutume de dire que dans le cyberespace, il est toujours plus difficile de défendre que d'attaquer. En effet, l'attaquant n'a souvent besoin que d'une seule faille pour arriver à pénétrer un système d'information, alors que le défenseur doit s'attacher à combler toutes les vulnérabilités. Pour autant, l'exemple de l'Ukraine a démontré qu'il n'existe pas de fatalité pour les défenseurs. Grâce à des investissements techniques et humains importants dans sa cybersécurité, l'Ukraine résiste aujourd'hui à des vagues toujours régulières de cyberattaques russes, qu'elle continue de subir.

La nécessité de devoir s'adapter à une menace plus massive se double en outre, dans le cyberspace, de celle de devoir suivre les évolutions technologiques. Dans le domaine technologique, l'intelligence artificielle connaît des évolutions incroyables depuis quelques mois ; elle est évidemment porteuse de risques nouveaux, au bénéfice des attaquants qui cherchent dès à présent à s'en servir, notamment pour automatiser ou démultiplier leurs attaques.

Mais l'IA offre aussi des opportunités nouvelles pour les défenseurs, afin d'améliorer la détection des attaques informatiques, la sécurité des codes informatiques que nous utilisons dans nos systèmes d'armes, dans nos systèmes de commandement ; mais aussi pour démasquer des manipulations de l'information. Selon moi, il ne s'agit pas tant de savoir à qui l'IA bénéficiera le plus, mais plutôt de disposer de modèles d'IA et de capacités de calculs performants, pour pouvoir en tirer pleinement profit. L'Agence ministérielle pour l'intelligence artificielle de défense (Amiad) nous aide à relever ce défi majeur pour les armées.

L'autre grande évolution technologique à venir, à fort impact, porte évidemment sur l'ordinateur quantique. Son avènement n'est pas encore clair, mais nous savons qu'il permettra, à un moment ou à un autre, de casser des codes cryptographiques aujourd'hui réputés comme inviolables. Ce risque est identifié depuis longtemps et bien pris en compte, notamment par la DGA, dans les équipements de chiffrement que nous utilisons pour protéger nos communications.

Pour conclure, face à des attaques dans le cyberspace, nos armées sont actives dans le combat. Il n'y a pas de fatalité ; nous pouvons nous défendre, comme l'Ukraine nous le démontre chaque jour. Il s'agit d'une nécessité absolue si nous voulons continuer à commander, à opérer et à gagner le combat dans le cyberspace, mais aussi sur terre, sur mer, dans l'air et dans l'espace.

M. le général de division Patrick Touak, chef du commandement du ministère de l'Intérieur dans le cyberespace. Le Comcyber du ministère de l'Intérieur est moins connu que le Comcyber des armées. Je m'attacherai donc à vous le présenter, avant de dresser un tableau de l'état de la menace et d'évoquer le sujet du numérique, à la fois en tant que menace de la part de nos adversaires, mais également en tant qu'opportunité pour le ministère de l'Intérieur.

Le Comcyber du ministère de l'Intérieur est jeune, puisque sa création remonte au 23 novembre 2023. Il s'agit d'un service ministériel commun à la police et à la gendarmerie nationales, dont la mission consiste à lutter contre la cybercriminalité. Nous formons particulièrement nos enquêteurs sur la criminalité cyber générale, mais surtout pour les enquêtes sous pseudonyme, notamment pour débusquer les pédocriminels. Nous les formons également à la lutte contre le blanchiment du produit des crimes et délits par l'utilisation de cryptoactifs.

Le deuxième pilier concerne la stratégie ministérielle. Le service est chargé de la définir – nous l'avons fait il y a presque deux ans – et surtout de la mettre en œuvre, à travers des mesures concrètes. Enfin, l'anticipation est essentielle : nous produisons des notes de renseignement complémentaires. La dimension prévention est également indispensable, compte tenu des dégâts durables occasionnés par la cybercriminalité, notamment en termes de fuites de données.

Face à ces menaces, une communauté d'acteurs est mobilisée : le Comcyber, l'Anssi, le GIP Cybermalveillance (ACYMA), Viginum, mais aussi le parquet, en particulier la section J3 Cybercriminalité du parquet de Paris. En effet, les enquêtes menées par les services de police et de gendarmerie s'inscrivent naturellement sous l'égide de ce parquet J3. Enfin, il faut naturellement citer la DGSI, dans son périmètre propre.

S'agissant de l'état de la menace, je rappelle fréquemment que la cybercriminalité se distingue par une caractéristique spécifique : elle peut s'exercer intégralement à l'extérieur du territoire national. Cette réalité impose nécessairement une coopération internationale renforcée, de nature opérationnelle, notamment avec Europol ; ou dans le cadre réglementaire et juridique, au niveau de l'Union européenne.

En effet, nos adversaires utilisent systématiquement les angles morts des législations nationales pour empêcher leur identification, la récupération de données ou leur interpellation. Cette coopération nous permet également d'accéder à des financements européens. Nous avons d'ailleurs pu acquérir des matériels utiles à nos enquêteurs grâce au fonds de sécurité intérieure.

La cybercriminalité ne cesse d'augmenter. Notre rapport annuel, décliné également en plusieurs langues (anglais, espagnol, arabe), précise que cette hausse atteint 87 % sur les cinq dernières années. Ce chiffre recouvre deux réalités : d'une part, une augmentation effective du phénomène liée à l'usage croissant du numérique ; et d'autre part, une augmentation du nombre de plaintes déposées par les victimes, qu'il s'agisse de personnes physiques ou d'entreprises.

Cette criminalité touche davantage que la criminalité ordinaire les personnes physiques. Je pense naturellement aux harcèlements, mais aussi aux escroqueries. Derrière la dimension financière, l'impact humain est particulièrement fort. Lorsqu'un comptable effectue un virement bancaire à la suite d'une escroquerie, l'élément psychologique est déterminant ; il a le sentiment d'avoir mis en péril son entreprise.

La majorité des attaques correspond à ce que l'on appelle les attaques par déni de service, les DDoS. Leur objectif consiste à saturer un site internet, souvent marchand, soit parce qu'il s'agit d'un concurrent, soit au titre de l'hacktivisme. Sur les 1347 revendications ou annonces de cyberattaques visant la France, recensées par le COMCYBER-MI en 2025, ces attaques s'élèvent à 53 %. Viennent ensuite les fuites et les ventes de données, sujet particulièrement marquant en 2025. Du point de vue du défenseur, la difficulté est structurelle : il suffit à l'assaillant de trouver une faille, quand il revient au défenseur de minimiser au maximum l'impact d'une intrusion. Les fuites de données constituent ainsi un enjeu central des deux dernières années, sur lequel nous devons continuer de travailler. Les rançongiciels représentent une autre composante majeure. Il s'agit pour les délinquants de chiffrer des

données, afin d'obtenir une rançon, mais aussi de plus en plus de les copier, les données ayant acquis une valeur économique considérable.

Une caractéristique forte des années 2025 et 2026 réside dans la porosité croissante entre les hackers et la criminalité organisée classique. Leurs profils sont parfois inattendus : certains jeunes, initialement animés par des logiques de défi, peuvent progressivement entrer en contact avec la criminalité organisée classique. Cette porosité s'étend également à des formes d'hacktivisme ou à l'exploitation par des acteurs étatiques de compétences techniques rares à des fins de déstabilisation ou de désinformation.

Un exemple concret peut être précisé en ce qui concerne les cryptomonnaies. Une fuite de données, initialement anodine, peut conduire à la constitution de listes d'individus. Pour la criminalité organisée, elle permet de cibler précisément des personnes, d'obtenir leurs coordonnées, leur activité et même le niveau de leurs avoirs, et ensuite de les séquestrer à leur domicile. Le vecteur cyber apparaît ainsi central dans des actes relevant par ailleurs de la criminalité traditionnelle.

Les escroqueries, notamment les « fermes à *scam* » ou « *scam centers* », constituent un autre phénomène majeur. Localisés en Asie du Sud-Est et souvent liés à la traite des êtres humains, ces dispositifs reposent sur des individus contraints de mener des escroqueries à distance. L'intelligence artificielle a profondément transformé cette pratique. Là où la maîtrise de la langue de la victime était auparavant nécessaire, il est désormais possible de traduire instantanément, permettant d'agir à grande distance sans connaissance linguistique préalable. Ce phénomène se développe de manière considérable et engendre des dégâts financiers, mais aussi psychologiques, très importants.

L'intelligence artificielle représente une évolution majeure. Elle ne crée pas de nouvelles formes de délinquance, mais facilite, professionnalise et accroît la nuisance des attaques. Elle permet notamment de produire des documents frauduleux extrêmement crédibles, tels que des avis de contravention, de fausses réquisitions. Pour s'en prémunir, il est recommandé aux entreprises de mettre en place des processus internes robustes, notamment pour les mouvements bancaires, afin de limiter les risques d'escroquerie, d'autant que les scénarios sont de plus en plus sophistiqués. Nous avons pu le constater lors de certains « cryptorapts ».

Cette porosité entre intelligence artificielle et cybercriminalité se manifeste également par l'apparition de services accessibles sur le *dark web*, permettant de louer ou de générer des outils d'attaque. Il est désormais possible d'obtenir automatiquement du code sans compétences techniques préalables. Cette accessibilité favorise la multiplication d'attaques, même de faible sophistication.

Un autre enjeu, plus minoritaire, mais significatif, concerne les faits de cyber-espionnage par intrusion dans les systèmes de traitement automatisé de données, qui ciblent notamment les sous-traitants d'entreprises de la base industrielle et technologique de défense (BITD) ou de bases militaires. Ainsi, lorsqu'un sous-traitant est victime d'une attaque, il est essentiel qu'il en informe les autres acteurs concernés, afin de prévenir d'éventuels effets de rebond.

Enfin, face à ces menaces, les autorités développent des réponses adaptées. Le ministère de l'Intérieur accorde une importance particulière à ces enjeux, notamment en matière de formation. Des centaines de policiers et de gendarmes sont formés chaque année, ainsi que des magistrats, avec lesquels une coopération étroite est entretenue. Par ailleurs, des formations sont dispensées à des polices étrangères, le centre de Lille bénéficiant d'une reconnaissance internationale, notamment grâce à des enseignements en langue anglaise.

Cependant, nous sommes parfois bloqués par le cadre réglementaire, qui nous empêche de profiter pleinement de ces technologies. Nous pouvons par exemple utiliser l'IA pour piéger un pédocriminel, en nous faisant passer pour un enfant. Cela signifie concrètement que nos enquêteurs peuvent transformer leur voix, leur image ; la loi nous le permet. Nous employons également l'intelligence artificielle pour la transcription. Notre procédure étant écrite, nous enregistrons les auditions, notamment celles des mineurs, et nous utilisons l'IA pour les retranscrire, afin de gagner du temps utile pour l'audition, pour l'enquête et pour d'autres activités.

Toutefois, je souhaite évoquer des usages qui ne sont pas autorisés et qui, pourtant, pourraient nous être utiles. Vous connaissez tous le dispositif « Alerte-Enlèvement », qui peut être déclenché lors de l'enlèvement d'un enfant, si le magistrat le décide, en fonction de certains critères. Il a prouvé son efficacité, puisque dans la quasi-totalité des cas, l'enfant est retrouvé sain et sauf grâce à la diffusion de sa photographie ou de celle de son kidnappeur.

Malheureusement, aujourd'hui, nous ne pouvons pas utiliser la reconnaissance faciale en temps réel *via* les systèmes de vidéoprotection de l'espace public, même dans un cas aussi circonscrit, pour identifier cette personne si elle passe devant une caméra. Nous diffusons pourtant sa photographie à grande échelle, mais il n'est pas possible d'exploiter un système qui vérifierait uniquement les visages correspondants, sans enregistrer l'ensemble des flux. Le dispositif « Alerte-Enlèvement » existe, il est efficace. L'intelligence artificielle pourrait en constituer un complément, mais nous ne pouvons pas l'employer, aujourd'hui.

Je souhaite également évoquer un deuxième exemple important, celui des fichiers judiciaires, tels que le traitement des antécédents judiciaires (TAJ) ou le fichier des personnes recherchées (FPR). Ces fichiers fonctionnent à partir d'une identité dite « NPDL », c'est-à-dire le nom, le prénom, la date et le lieu de naissance. Ainsi, certaines personnes indiquent ne pas avoir de document lorsqu'elles sont contrôlées et déclarent de fausses identités, s'engouffrant dans une brèche.

Il existe un autre fichier, le fichier automatisé des empreintes digitales (Faed), qui permet d'identifier une personne avec une grande fiabilité, par son empreinte digitale. Cependant, ce fichier n'est pas connecté aux autres traitements, ce qui empêche de fusionner les informations. Cela constitue un frein réglementaire, alors même que ce type d'interconnexion existe chez certains de nos voisins européens. Une telle évolution nous permettrait, dans certains cas, de retrouver des individus recherchés, inscrits dans ces fichiers judiciaires par décision de justice, et de préserver des vies humaines.

Enfin, je souhaite évoquer un dernier point relatif à des contrôles d'identité évoqués dans la presse. Dans l'exercice de leur mission, des policiers ont utilisé la reconnaissance faciale en dehors du cadre légal, en utilisant leurs téléphones pour transmettre à leurs collègues des photographies des individus interpellés et ne disposant d'aucun papier d'identité, et ce aux fins

de comparaison avec les photographies de mis en cause enregistrées dans le TAJ. Pourtant, lorsque des individus déclarent ne pas avoir de documents, cet outil pourrait être utile pour vérifier s'ils sont recherchés. Ce dispositif existe, mais uniquement dans une procédure judiciaire. L'utilisation de ces nouvelles technologies dans un cadre administratif, dont les contours seraient définis par le législateur, serait utile, dans le but de protéger la population, gagner du temps, mieux travailler.

En conclusion, face à une cybercriminalité qui évolue constamment, le criminel conserve un temps d'avance car il ne respecte ni les règles, ni les lois. Nous ne pouvons donc que réagir avec un temps de retard, et nous avons besoin du législateur pour mieux utiliser ces technologies. L'intelligence artificielle ne sert qu'à une chose : gagner du temps pour le consacrer à des missions plus essentielles.

M. le président Jean-Michel Jacques. Je vous remercie pour ces propos nourris et cède la parole aux orateurs de groupe.

M. Laurent Jacobelli (RN). Au nom du groupe Rassemblement National je vous remercie pour les explications que vous avez bien voulu partager avec nous et pour votre présence aujourd'hui. J'ai bien entendu vos remarques, qui permettent d'établir une comparaison entre les lourdeurs administratives que nous pouvons connaître dans notre pays et la rapidité qu'impose ce type de cyberattaque ou de cybercriminalité. Un autre sujet m'est également venu en tête concernant ces fameuses lourdeurs. Dans ce domaine du cyber, il existe en France de nombreux organismes, de nombreux services. Au-delà des deux vôtres, il faut ainsi mentionner l'Anssi et Viginum par exemple. Ces agences ne sont-elles pas trop nombreuses ? Cette multiplication n'entraîne-t-elle pas une trop grande dispersion de l'analyse et de la décision ?

Ne pourrait-on pas gagner en rapidité, en coordonnant ces services de manière plus précise ? Considérez-vous au contraire que ces diverses agences constituent une source de richesse, de complémentarité et d'efficacité ? J'aimerais recueillir votre avis, dans un secteur où il faut être rapide, où la fluidité compte et où les attaques peuvent être réalisées à moindre coût par un grand nombre d'individus.

Ensuite, jamais les questions militaires et civiles n'ont été aussi proches. De fait, une attaque cyber qui cible notre secteur énergétique, notre système bancaire ou notre système hospitalier, peut paralyser la France. Ce type d'attaque peut engendrer un effet majeur et nécessite que nous fassions preuve de réactivité et de rapidité. En sommes-nous capables ?

Deuxièmement, une coopération avec certains pays européens – plutôt que dans le cadre général européen – peut-elle être utile ? À l'inverse du Système de combat aérien du futur (Scaf), il ne s'agirait pas de quelque chose d'idéologique, mais d'une démarche pratique et réellement concrète.

Enfin, il existe aussi une « guerre des satellites » entre les différentes options disponibles. L'Italie serait intéressée par la solution d'Elon Musk plutôt que par la solution française. Quels risques percevez-vous dans ce domaine ?

M. le général de division aérienne Emmanuel Naëgelen. Concernant l'écosystème des agences ou des entités, je rappelle d'abord que, si nous sommes plusieurs acteurs, nos missions demeurent très distinctes. L'Anssi exerce une mission uniquement

défensive, tandis que, pour ma part, j'assume une mission offensive, ce qui justifie l'existence d'organisations séparées. Toutefois, des structures de coordination interministérielle existent et fonctionnent de manière pleinement opérationnelle, notamment le C4 et le Colmi. Le C4 constitue ainsi une organisation permanente. Les échanges sont continus entre techniciens chargés de l'analyse technique continue de la menace.

Cette fluidité représente d'ailleurs un atout majeur, souvent envié par nos homologues européens, qui ne disposent pas d'un tel niveau de coordination entre les différentes entités de l'État participant à la cybersécurité et la cyberdéfense. En parallèle, l'action européenne constitue également un volet essentiel pour les armées. À ce titre, nous avons mis en place un forum des cyber commandeurs européens, une initiative française, visant notamment à renforcer la coordination – ce qui se déroule en Allemagne et en Pologne peut très rapidement se propager en France, en raison de l'interconnexion des réseaux. J'entretiens d'ailleurs des relations très cordiales et très amicales avec l'ensemble de mes homologues européens. Enfin, ce cadre favorise également l'accompagnement de certains partenaires européens dans la montée en maturité de leurs capacités cyber.

M. le général de division Patrick Touak. Je partage pleinement ces propos, tout en rappelant que nous intervenons de manière complémentaire sur des sujets distincts, en maintenant des échanges réguliers. Dès lors qu'une infraction est caractérisée, qu'une plainte est déposée ou qu'une enquête peut concerner directement le périmètre des armées, nous nous coordonnons immédiatement. Des protocoles existent et des structures de partage d'informations sont établies. L'essentiel réside dans l'échange de renseignement et dans la compréhension des techniques de l'adversaire, ainsi que des réponses que nous pouvons y apporter.

Au sein du ministère de l'Intérieur, notre action se déploie sur deux volets, en complément de l'Anssi, qui définit la sécurité des systèmes d'information au niveau national. La police et la gendarmerie apportent, pour leur part, une force d'ancrage territorial. À l'échelle départementale et régionale, le lien avec les délégués régionaux de l'Anssi permet d'agir en matière de prévention cyber, notamment auprès des collectivités, des TPE et des PME.

Au niveau européen, la coopération cyber, de très grande qualité, s'appuie notamment sur Europol. Elle doit s'accompagner d'une veille juridique indispensable pour détecter les angles morts, particulièrement dans le domaine cyber, où la délinquance peut s'exercer sans présence physique sur le territoire national.

M. Karl Olive (EPR). Au nom du groupe Ensemble pour la République, permettez-nous de vous remercier pour vos interventions, particulièrement éclairantes, glaçantes parfois, sur les sujets qui figurent désormais au cœur de notre souveraineté et de notre sécurité. Ainsi que vous l'avez indiqué, la cyberdéfense ne concerne pas seulement nos armées, mais touche également nos administrations, nos collectivités, nos entreprises, nos infrastructures critiques et, au fond, la sécurité quotidienne des Français.

Cette audition intervient au cours d'une séquence importante, alors que le Sénat a rejeté l'article 2 de l'actualisation de la loi de programmation militaire (LPM) qui prévoyait 36 milliards d'euros supplémentaires pour nos armées sur la période de 2026-2030. Je tiens d'ailleurs à rappeler ici que nous défendrons fermement le rétablissement de cette

trajectoire budgétaire. Dans le contexte international actuel, l'effort de défense ne peut pas être une variable d'ajustement.

Du 15 au 17 juin prochain, la France accueillera également le sommet G7 à Evian. Ce rendez-vous international majeur impose une vigilance renforcée face au risque d'espionnage, de déstabilisation, d'ingérence et de manipulation de l'information. Le président de la République l'a rappelé le 3 octobre dernier à Sarrebruck, à l'occasion du trente-cinquième anniversaire de la réunification allemande.

La guerre revient sous toutes ses formes, notamment hybrides, par exemple à travers les manipulations de l'information. Les chiffres le confirment : 1 366 incidents ont été portés à la connaissance de l'Anssi en 2025 et 453 200 crimes et délits liés au numérique ont été enregistrés la même année par le ministère de l'intérieur.

Les opérations militaires dépendent très directement d'infrastructures civiles : les télécommunications, l'énergie, les transports, les prestataires informatiques ou encore les sous-traitants industriels. Dans l'hypothèse d'une crise majeure ou d'un conflit de haute intensité, comment s'assurer qu'une cyberattaque visant un acteur civil ne vienne pas fragiliser directement notre capacité opérationnelle militaire ?

M. le général de division aérienne Emmanuel Naëgelen. Lors de mon propos liminaire, j'ai abordé notre dépendance aux fournisseurs et aux infrastructures critiques nécessaires au fonctionnement de nos armées. Ce sujet est anciennement identifié et a conduit à une première réponse, dans le cadre d'une LPM assez ancienne : la protection de ces infrastructures critiques, non seulement pour les armées, mais pour la nation tout entière. C'est dans ce cadre que des dispositifs législatifs ont permis à l'Anssi de travailler avec les opérateurs d'importance vitale (OIV) afin de garantir la sécurité de leurs systèmes d'information, indépendamment de leurs liens avec les armées. L'Anssi mène ce travail depuis de nombreuses années, notamment pour les domaines « hyper critiques » de l'énergie et des télécoms, où le niveau de sécurité atteint est aujourd'hui très robuste.

Cette solidité a été éprouvée lors des Jeux olympiques, en amont desquels un grand nombre d'exercices et d'évaluations avaient été menés, produisant des conclusions rassurantes. Force est de constater que pendant les JO, aucune attaque n'a produit d'effet significatif sur ces opérateurs. Conscients des risques associés à l'importance de leurs activités, les OIV se sont organisés pour mettre en place une cybersécurité robuste.

Toutefois, la difficulté réside désormais dans l'extension de cette sécurité à l'ensemble des nombreux sous-traitants et fournisseurs. Dans ce cadre, un travail de fond est conduit par les grandes entreprises elles-mêmes, mais également au sein du ministère des armées.

Les armées ont également recours à un très grand nombre de fournisseurs. À ce titre, nous menons un vaste chantier, avec l'appui de la direction du renseignement et de la sécurité de la défense (DRSD) pour les marchés classifiés, y compris auprès de petites entreprises ; mais aussi celui de la direction générale de l'armement (DGA) pour les fournisseurs de l'armement ; et de tous les autres organismes du ministère ayant recours à ces fournisseurs. Nous œuvrons ardemment à la sécurisation des fournisseurs du ministère des armées.

M. le général de division Patrick Touak. La menace cyber a été intégrée dès l'origine dans le cadre du G7. Nous avons ainsi procédé à un état précis de la menace et organisé une participation active visant à anticiper, grâce au renseignement et à la veille, tout en étant prêts à agir avec nos partenaires. Cette anticipation inclut également les risques d'ingérence, qu'il convient d'identifier en amont, puisqu'ils participent à des stratégies de déstabilisation du pays. Comme pour toute criminalité, le risque zéro n'existe pas, ce qui impose de développer une véritable culture du numérique fondée sur la détection rapide des attaques.

Dans le cadre de la prévention, nous expliquons aux collectivités, mais aussi aux entreprises – petites et grandes – qu'il faut réduire l'impact de l'attaque au maximum. À l'instar des doctrines appliquées à d'autres menaces, il s'agit de ralentir et de contenir les effets d'une intrusion en mettant en place des mesures passives anticipées. Cela implique, par exemple, de limiter les conséquences d'une fuite de données par un agent corrompu. Les systèmes doivent ainsi être en mesure de détecter des anomalies et d'alerter rapidement.

Enfin, cette démarche repose sur une chaîne cohérente articulant détection, réduction de l'impact, remédiation et retour d'expérience. L'humain demeurant une vulnérabilité potentielle, il est indispensable d'intégrer pleinement cette dimension dans la stratégie globale, afin de maîtriser au mieux les effets d'une attaque.

Il faut développer cette culture de détection de l'alerte. Quel que soit le niveau de sécurité informatique ; l'humain reste la faille, qu'il s'agisse de corruption, de compromission, de menaces sur la famille, enfants ou conjoints. Encore une fois, il s'agit d'abord de mieux détecter, de réduire l'impact et de cultiver le retour d'expérience.

M. Arnaud Saint-Martin (LFI-NFP). Messieurs les généraux je souhaiterais obtenir votre éclairage sur une question *a priori* latérale, mais au cœur de l'actualité récente : la dissuasion spatiale.

Les systèmes spatiaux sont indispensables à nos sociétés et constituent une infrastructure matérielle critique du cyberespace. Ils viabilisent les télécommunications, la navigation, la télédétection, le renseignement, les opérations de défense la météo ou encore la surveillance du climat. Or, récemment, Josef Aschbacher, le directeur général de l'Agence spatiale européenne (ESA), a déclaré dans la presse que la perte de ses capacités constituerait « *le pire scénario imaginable, non seulement pour la défense, mais aussi pour la vie quotidienne de chaque citoyenne et citoyen* ». Il ajoutait qu'une attaque majeure contre les infrastructures spatiales au sol ou sur orbite circumterrestre pourrait engendrer un impact systémique, comparable par son ampleur, à celui d'une attaque nucléaire.

Depuis une dizaine d'années Jean-Luc Mélenchon et La France insoumise alertent sur la vulnérabilité de nos infrastructures stratégiques sous l'angle de la dissuasion spatiale laquelle désigne pour dire vite la capacité à désorganiser un pays tout entier par une attaque sur ses satellites ou ses segments sol par divers moyens. L'exemple de l'attaque contre le réseau satellitaire Viasat en Ukraine en 2022 a montré qu'il est possible de désorganiser simultanément des communications militaires et civiles à grande échelle.

Par ailleurs, la Chine, l'Inde, les États-Unis et la Russie ont démontré leurs capacités antisatellites. La France accuse le coup, mais surtout un préoccupant retard au niveau spatial, mais aussi de ses segments sol exposés aux menaces et attaques.

Il s'agit non pas d'une logique de militarisation aveugle et infinie de l'espace, mais de la capacité de rendre toute attaque contre nos infrastructures spatiales suffisamment coûteuses pour décourager un adversaire. Il convient ainsi de protéger nos infrastructures, de disposer de capacités de remplacement de nos satellites, de protéger nos segments sol, aujourd'hui les plus vulnérables aux attaques cyber.

Dès lors, considérez-vous que la France dispose actuellement des capacités défensives et offensives nécessaires pour préserver, prévenir et empêcher qu'une puissance étrangère ou même un acteur privé puisse désorganiser notre société tout entière ? Sommes-nous préparés, le cas échéant, aux conflits spatiaux qui s'annoncent ?

M. le général de division aérienne Emmanuel Naëgelen. Vous avez cité l'exemple de l'Ukraine et de Viasat, que nous avons suivi avec un très grand intérêt, d'autant plus que cet événement a provoqué des répercussions en France. Certains services assurés par cette entreprise de communication par satellite ont été indisponibles dans plusieurs pays européens, y compris sur notre territoire, ce qui montre que l'impact a dépassé largement le seul cadre ukrainien. Cette situation a mis en lumière le fait que, dans un contexte de conflit, les systèmes satellitaires de communication peuvent être ciblés par des attaques informatiques.

Même si les effets n'ont pas été aussi critiques qu'ils auraient pu l'être, cela demeure un enjeu majeur, en particulier pour les armées qui utilisent ces systèmes satellitaires pour la communication, la navigation et l'observation. C'est pourquoi un Commandement de l'espace (CDE) a été créé, afin de disposer d'une vision globale de ces capacités satellitaires, de leur protection et de l'organisation d'éventuels combats dans l'espace. Nous disposons de relations très étroites avec ce CDE, à double titre. Il s'agit d'une part de l'aider dans la défense de ses infrastructures de ses systèmes ; mais aussi d'imaginer comment, en tant que militaires, nous pourrions développer des capacités offensives sur des systèmes satellites.

Naturellement, nous réfléchissons à ces sujets, même si je ne peux répondre de manière plus précise sur ce sujet hautement sensible. Toutefois, les communications ne reposent pas uniquement sur les satellites, mais aussi sur les câbles, les fibres optiques, et les systèmes de type radio. L'enjeu central reste donc la résilience globale des communications, face aux menaces cyber et aux actions de guerre électronique de type brouillage, comme on l'observe sur le théâtre ukrainien, afin de maintenir en permanence le lien entre les postes de commandement et les unités. Le sujet est complexe, mais nous y travaillons tous les jours.

Mme Anna Pic (SOC). Récemment, nous avons appris que Tchap, la messagerie officielle de l'administration française, avait été victime d'une cyberattaque. Je veux d'abord saluer la réactivité des services concernés, notamment la direction interministérielle du numérique (Dinum) et l'Anssi, qui ont rapidement identifié l'incident et engagé les mesures nécessaires.

Néanmoins, les chiffres avancés questionnent, car Tchap n'est pas une messagerie ordinaire. Il s'agit d'un outil de confiance de l'État, utilisé par les agents de ministères régaliens, comme les ministères de l'intérieur, des armées, de la justice, des finances, ou de l'éducation nationale. Ainsi, 73 000 agents seraient potentiellement concernés, soit plus de 640 000 messages, près de 60 000 fichiers médias et presque trois années d'échanges internes. Si des documents partagés, des liens de visioconférence ou des informations liées à

des activités sensibles ont pu être accessibles, nous sommes face à un enjeu de sécurité opérationnelle.

Quelles mesures immédiates ont-elles été prises pour contenir le risque de diffusion, notamment en matière d'authentification, d'information des agents concernés, de vérification des accès ? Au-delà de la solution à court terme, envisagez-vous un renforcement plus structurel de Tchap ou un changement de messagerie ? Comment mieux informer les élus sur les questions de sécurité dans nos messageries ?

Êtes-vous en mesure d'évaluer l'étendue et l'impact de la diffusion de certaines informations particulièrement sensibles ? Comment y faire face ? Enfin, quelles conséquences tirez-vous de cet incident pour la doctrine d'emploi des messageries sécurisées de l'État, afin d'éviter que cet incident ne se reproduise ?

M. le général de division Patrick Touak. La fuite de données sur Tchap s'inscrit d'abord dans une série d'événements, sans qu'il soit possible, à ce stade, de fournir des éléments concrets supplémentaires. En termes d'impact précis, je ne dispose pas d'informations spécifiques au-delà de celles rendues publiques. Il convient néanmoins de rappeler que, lors de ce type d'attaque, une obligation légale impose d'informer les personnes concernées. Parallèlement, des enquêtes sont engagées, tant judiciaires et des mesures techniques sont mises en œuvre, afin d'éviter que les faits ne se reproduisent.

Il faut ensuite envisager que le risque d'intrusion subsiste en permanence. Il est difficile de prévoir l'intégralité des attaques, et une seule peut suffire. Dès lors, il devient essentiel de développer une culture du retour d'expérience, afin de comprendre les mécanismes à l'origine de l'incident. Il peut ainsi s'agir d'une erreur humaine. Au-delà, dès qu'elles ont connaissance d'une intrusion, d'un compte compromis, les entreprises doivent avoir le réflexe de remonter immédiatement l'alerte, pour tous les systèmes sensibles. Certes, il est parfois délicat de déterminer où placer le seuil, mais il faut reconnaître que des attaques surviendront encore. La question est donc de savoir comment les détecter, comment en limiter l'impact, puis comment assurer la remédiation.

À cet égard, je souhaite évoquer, à titre d'exemple, le fichier TAJ, qui a été victime d'une attaque au mois de décembre dernier. Des mesures concrètes ont été prises. D'abord, pour nos agents, l'authentification forte a été généralisée : désormais, l'accès se fait avec la carte professionnelle et non plus par un simple identifiant et mot de passe. Ensuite, des mécanismes d'alerte ont été instaurés. Lorsqu'un nombre de consultations paraît anormal au regard de l'affectation, une alerte est déclenchée et fait l'objet d'une vérification.

Mme Valérie Bazin-Malgras (DR). Ma question porte sur le champ de bataille de l'information. En effet, le XXIe siècle est marqué par la montée en puissance de la guerre hybride. Les manipulations de l'information constituent, dans ce cadre, une arme de guerre qu'il ne faut pas négliger. À partir d'une simple description, l'IA générative est capable de fabriquer des images d'un réalisme inquiétant. En manipulant ainsi des images, de telles réalisations pourront décupler les capacités de désinformation de puissances hostiles.

Une réalité alternative pourra être ainsi créée pour servir des motivations stratégiques par nature préoccupantes, car elles reposent sur le mensonge. Les campagnes de désinformation menées par la Russie en Afrique subsaharienne ont fortement contribué à des renversements de régime. Où en sont nos forces armées dans le développement de capacités de

lutte sur le champ de bataille de l'information ? Au-delà de l'outil Viginum, nos armées se dotent-elles de capacités offensives dans ce domaine ?

M. le général de division aérienne Emmanuel Naëgelen. Aujourd'hui, aucun conflit ne se déroule sans s'accompagner d'une véritable bataille des narratifs, devenue de plus en plus marquée et ouverte. Cette réalité, d'abord observée en Afrique, s'est désormais généralisée à l'ensemble des conflits contemporains. Les armées se sont ainsi organisées dans une approche globale, en considérant que cette bataille relève à la fois du cyber et du technique, mais surtout du narratif et de l'influence. En lien étroit avec le Quai d'Orsay, nous avons mis en place un cadre, afin de porter et faire connaître le narratif français, relayé notamment par les ambassadeurs, permettant d'opposer le contre-narratif de la France.

Sur le plan technique, il s'agit ensuite de comprendre ce qui se joue sur les réseaux sociaux et les sites *web*. Les armées ont développé des capacités de détection, afin d'identifier la désinformation et d'en mesurer l'impact, qu'il s'agisse d'un phénomène marginal ou d'une diffusion plus large. Des outils, également utilisés dans le secteur privé pour la gestion de la réputation, permettent d'assurer cette veille. Les armées sont évidemment organisées pour être en mesure de détecter très rapidement toute atteinte à leur réputation.

Détecter ouvre également la possibilité de répondre. Le chef d'état-major de l'armée de Terre ou d'autres de nos grands chefs ont pris la parole publiquement pour rétablir la vérité, par exemple, sur un certain nombre de désinformations, de manipulations de l'information. De fait, la première réponse consiste ainsi à rétablir la vérité des faits, simplement.

Enfin, un volet offensif existe, dans le cadre de ce que j'appelle « la lutte informatique d'influence », afin de pouvoir tromper nos adversaires, en cas de conflit. Ces actions ne constituent pas des nouveautés ; elles relèvent de la ruse, de la « déception », parties intégrantes de l'art de la guerre.

M. le général de division Patrick Touak. Madame la députée, vous avez évoqué la lutte informationnelle face à la désinformation, qui, sans constituer formellement une criminalité qualifiée, représente néanmoins une menace majeure, y compris sur le territoire national. Ce risque s'est particulièrement illustré lors des élections, notamment municipales, où des dispositifs comme Viginum ont été mobilisés. Il s'agit d'un enjeu essentiel pour la stabilité de notre démocratie, comme en témoignent certains cas européens où des processus électoraux ont été déstabilisés, voire annulés.

Ce défi est aujourd'hui accentué par le développement de l'intelligence artificielle, qui facilite l'accès immédiat à l'information, là où les générations précédentes ont été formées à la recherche, à la mémorisation et à l'effort. Dès lors, un enjeu collectif s'impose : réintroduire à l'école le goût de l'effort, y compris l'effort « inutile », et développer l'esprit critique. Face à une information potentiellement altérée, seule la capacité à raisonner de manière autonome permet d'éviter les manipulations.

M. Damien Girard (EcoS). En matière de cybersécurité, la France dispose d'un corpus stratégique parmi les plus développés en Europe. La stratégie nationale de résilience de 2022, la revue nationale stratégique (RNS) de 2025, puis la stratégie nationale de cybersécurité 2026-2030 ont progressivement fait de la cyberrésilience une priorité de sécurité nationale. Cet effort mérite d'être souligné. La France a été pionnière, avec la réglementation des opérateurs

d'importance vitale et a joué un rôle moteur dans l'élaboration des directives européennes, NIS, puis NIS 2.

Mais ce volontarisme stratégique contraste avec certaines réalités. La France est en effet l'un des États membres qui n'a toujours pas transposé la directive NIS 2, alors même que la date limite était fixée au 17 octobre 2024. Nous sommes pourtant parmi les pays les plus exposés aux cyberattaques en Europe. Quel risque ce retard fait-il peser sur nos administrations, nos entreprises et nos collectivités ?

Je m'interroge également sur la gouvernance même de notre politique de cybersécurité. L'État produit des stratégies de qualité, identifie des menaces et fixe les objectifs ambitieux. Aujourd'hui, la question n'est plus celle de la stratégie, mais celle de l'exécution. Quels sont les investissements réellement consacrés à la cybersécurité dans l'ensemble des ministères ? Quels indicateurs permettent-ils d'évaluer des progrès accomplis ? Existe-t-il un tableau de bord interministériel partagé permettant de mesurer le niveau réel de protection de l'État ?

Enfin, je souhaiterais vous entendre sur le rôle de l'Anssi. Personne ne conteste aujourd'hui son expertise, ni la qualité de son travail, mais l'Agence peut-elle durablement exercer à la fois des missions opérationnelles, réglementaires, doctrinales et de coordination de l'ensemble des acteurs publics ? Dispose-t-elle de moyens humains et de l'autorité nécessaire pour imposer des standards communs à des administrations souvent attachées à leur autonomie informatique ? Autrement dit, au-delà de la qualité reconnue de l'Anssi, notre organisation institutionnelle est-elle aujourd'hui la mieux adaptée pour faire de la cybersécurité une véritable politique publique de transformation de l'État ?

M. le général de division Patrick Touak. Nous attendons effectivement la transposition de la directive NIS 2 en France. Pour autant, cela ne nous empêche pas d'agir dès à présent. L'Anssi a mis en place un formulaire permettant aux entreprises et aux collectivités de se déclarer, afin d'effectuer un recensement et de diffuser des conseils adaptés. En effet, si le périmètre exact dépendra des arbitrages définitifs, nous connaissons déjà les grandes orientations de la directive, ce qui nous permet d'engager des messages de prévention concrète. Ainsi, au quotidien, nous accompagnons les collectivités et les entreprises, en leur proposant des mesures de sécurité et des recommandations pour mieux faire face aux attaques.

Cette action s'inscrit en cohérence avec la stratégie nationale cyber et repose sur une coordination étroite avec l'Anssi, notamment grâce à son réseau de délégués régionaux. En complément, la police et la gendarmerie apportent un maillage territorial dense, permettant d'agir au plus près des acteurs locaux. Nos référents sûreté sont présents dans tous les départements.

Au-delà des aspects réglementaires, la question des investissements ne saurait être réduite à une dimension financière. L'enjeu principal réside dans les compétences, les ressources humaines. Il s'agit de développer une véritable filière numérique au sein des administrations, capable de recruter et former. Sans cette base, les investissements seraient insuffisants.

Par ailleurs, il nous faut sans doute des réglementations plus facilitatrices, car notre interprétation des règlements diffère de celle de certains autres pays européens. Je n'ai pas non plus identifié de tableaux de bord semblables à ceux que vous mentionniez. Nous assurons

néanmoins un suivi aussi précis que possible des obsolescences des systèmes. Sur ce point, la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic) ou les directions des systèmes informatiques des ministères seraient sans doute plus à même de vous répondre.

Les obsolescences sont suivies, notamment à travers les processus d'homologation. Il pourrait être pertinent, toutefois, de réduire un parc applicatif souvent étendu, fruit d'une succession de développements numériques et de marchés publics ayant conduit à des choix technologiques variés. Ces aspects militent en faveur d'un regroupement. Cependant, encore une fois, le défi est d'ordre RH, recruter et fidéliser les talents demeure essentiel. Il faut pouvoir les conserver et leur promettre au sein de nos administrations un déroulement de carrière à la hauteur de ce que le privé peut leur proposer.

M. le général de division aérienne Emmanuel Naëgelen. Nous bénéficions d'une loi de programmation militaire particulièrement ambitieuse sur le volet cyber, qui constitue une véritable chance pour les armées. Cette dynamique permet de consolider les fondamentaux identifiés dans la stratégie nationale cyber, parmi lesquels figurent notamment les équipements de chiffrement. Ces équipements, bien que peu visibles et souvent méconnus, sont absolument indispensables, car ils garantissent la protection de nos communications et empêchent nos adversaires d'y accéder librement. Ils constituent, en réalité, la base même de la cybersécurité, et le fait que la LPM prévoie un réinvestissement dans ce domaine représente une avancée majeure.

Par ailleurs, cette loi apporte également des ressources humaines supplémentaires, car la cyber ne repose pas uniquement sur des outils techniques, mais aussi sur des hommes et des femmes qualifiés. Néanmoins, nous faisons face à un défi qui dépasse largement le ministère des armées, c'est-à-dire une pénurie préoccupante de professionnels de la cybersécurité en France. Dans ce contexte, les armées se trouvent en concurrence directe avec d'autres acteurs sur le marché du travail.

Ainsi, si le recrutement demeure possible, notamment grâce à l'attractivité du métier militaire, la difficulté principale réside dans la fidélisation des talents. Les jeunes ingénieurs, après une première expérience, sont rapidement attirés par le secteur privé, où les rémunérations sont plus élevées. Il est donc impératif d'adapter nos modèles de ressources humaines pour répondre à cette contrainte, liée à l'insuffisance du nombre de professionnels de cybersécurité.

Mme Geneviève Darrieussecq (Dem). Vous avez parlé de sous-traitants, de fournisseurs, de points de vulnérabilité. Mais en réalité, chaque Français n'est-il pas potentiellement un point de vulnérabilité, en matière de cybersécurité ? Pensez-vous que la sensibilisation à la cybersécurité dès le plus jeune âge est aujourd'hui suffisante en France ? Les entreprises, administrations ou hôpitaux ne devraient-ils pas mettre en place des formations obligatoires pour chaque salarié dans ce domaine, afin de limiter progressivement les intrusions dans les systèmes, qui peuvent d'ailleurs relever d'infrastructures critiques ?

M. le général de division aérienne Emmanuel Naëgelen. Ce sujet est particulièrement important, notamment à travers le lien armée-jeunesse, même s'il dépasse ma seule responsabilité en tant que Comcyber. L'éducation nationale mène déjà des actions structurantes, notamment avec les certifications Pix, désormais obligatoires pour les collégiens

et les lycéens, qui les confrontent aux enjeux de cybersécurité et constituent une première étape essentielle.

Dans ce cadre, les armées ont cherché à renforcer cette dynamique en se rapprochant de l'éducation nationale. Nous avons ainsi lancé l'initiative « Passe ton hack d'abord », destinée à sensibiliser les lycéens à la cybersécurité à travers une approche ludique, que nous accompagnons. Cette action, initialement limitée à quelques centaines de participants, a connu une montée en puissance significative pour atteindre près de 10 000 participants récemment, ce qui témoigne de son succès et de l'intérêt suscité.

Parallèlement, la sensibilisation constitue déjà une obligation au sein des armées, incluant des formations et des rappels réguliers. Toutefois, ces dispositifs restent nécessaires, mais insuffisants, car les menaces évoluent rapidement. Il est facile de se faire piéger. Aujourd'hui, les techniques d'usurpation, notamment grâce à l'intelligence artificielle, rendent extrêmement difficile la détection de courriels frauduleux.

Dans ce contexte, il apparaît indispensable d'adapter les outils eux-mêmes. Les éditeurs de logiciels portent à ce titre une responsabilité et doivent faire en sorte que leurs logiciels soient plus faciles à sécuriser, plus robustes et plus simples d'usage, afin que la protection ne repose pas uniquement sur l'expertise des utilisateurs.

M. le général de division Patrick Touak. Le Comcyber-MI a mené, en lien avec l'éducation nationale, une opération intitulée « Cactus », qui vise à sensibiliser à la fois les élèves et les parents d'élèves. Cette campagne repose sur des techniques classiques de *phishing*, consistant à envoyer des courriels pour observer les réactions. Les résultats montrent malheureusement que les jeunes restent facilement vulnérables, car il suffit souvent de les attirer. Le *phishing* et le *smishing* demeurent donc des méthodes très efficaces, ce qui impose de multiplier les actions de sensibilisation.

Dans ce cadre, la question se pose ensuite de savoir s'il convient d'agir de manière nominative ou anonyme. Sans nécessairement sanctionner, il apparaît toutefois important d'identifier les comportements à risque récurrents afin d'adapter la prévention, car une simple erreur peut mettre en péril une entreprise ou une collectivité à travers une fuite de données.

Au-delà de la sensibilisation, il est indispensable de se préparer à l'attaque elle-même. Cela implique de développer une culture de la protection contre soi-même, comparable à celle des pilotes formés à apprendre par cœur et répéter des procédures en cas d'incident.

L'expérience du télétravail pendant le Covid a, par exemple, mis en évidence des vulnérabilités simples, comme l'usage d'ordinateurs professionnels par des enfants. Dès lors, il apparaît essentiel de renforcer les bonnes pratiques, tout en développant les capacités de détection des attaques et de réduction de leurs impacts, la seule sensibilisation ne suffisant plus face à des menaces amplifiées par l'intelligence artificielle.

M. Didier Lemaire (HOR). Ma question portera sur l'articulation entre vos deux commandements face à des menaces qui, par nature, refusent les frontières que nous traçons entre elles.

Le cycle qui nous réunit porte sur le *continuum* de conflictualité. Ce terme n'est pas qu'une commodité de langage, mais décrit une réalité opérationnelle. Une attaque qui se présente d'abord comme un acte de cybercriminalité, un rançongiciel sur un hôpital ou une intrusion dans le système d'une collectivité, peut en réalité dissimuler une logique de déstabilisation, voire la main d'un acteur étatique opérant par l'intermédiaire de *proxys*.

Inversement, une opération clairement hostile peut s'abriter derrière les apparences de la délinquance ordinaire pour entretenir le doute et compliquer l'attribution. Cette ambiguïté est précisément l'effet recherché par nos compétiteurs. Elle exploite nos lignes de partage administratif : d'un côté, le commandement des armées tourné vers l'agression extérieure et la conflictualité étatique ; de l'autre, le commandement du ministère de l'intérieur en première ligne sur la cybercriminalité et la protection, sur le territoire national. À cela s'ajoute l'Anssi, autorité de cybersécurité. Il existe donc trois acteurs, trois logiques pour une menace qui est continue.

Lorsqu'un incident émerge, sans que l'on sache encore s'il relève de la délinquance, de l'ingérence ou de l'agression, comment se prend concrètement la décision de qualification ? Qui en a la charge ? Existe-t-il aujourd'hui une chaîne de coordination suffisamment fluide entre vos deux commandements et l'Anssi pour réagir en temps réel ou demeure-t-il des zones grises de compétences que l'adversaire sait identifier et exploiter ? Si ces zones grises existent, quelle évolution de doctrine ou d'organisation, appelez-vous de vos vœux, pour les combler ?

M. le général de division aérienne Emmanuel Naëgelen. Pour améliorer la coordination, je bénéficie au sein de mon commandement de la présence d'un officier de gendarmerie issu du Comcyber du ministère de l'intérieur. Cette mesure concrète me permet d'être informé très rapidement en cas d'attaque visant un sous-traitant et d'en mesurer immédiatement les impacts potentiels sur les armées, soit un dispositif simple, mais pleinement efficace.

À un niveau plus global, la réponse repose sur le mécanisme de coordination du C4. Celui-ci fonctionne à plusieurs niveaux, à commencer par un niveau technique où, quotidiennement, des échanges ont lieu entre les techniciens. Mon centre expert en cyberdéfense collabore ainsi étroitement avec les équipes de l'Anssi, du ministère de l'intérieur, de la DGA et de l'ensemble des acteurs disposant de compétences techniques, pour caractériser la menace

Cette caractérisation exige de combiner des compétences techniques cyber, permettant d'analyser les modes opératoires, et des capacités de renseignement ou de police, afin d'attribuer l'attaque à des acteurs précis, par exemple un service de renseignement ou un acteur criminel. La difficulté tient notamment aux stratégies de dissimulation, les attaquants pouvant aisément usurper des identités en réemployant des outils existants pour faire croire à une autre origine. Dans ce contexte, le rôle des services de renseignement est essentiel pour lever ces ambiguïtés et déjouer les faux drapeaux.

M. le général de division Patrick Touak. Les relations existent au niveau central, mais les relations de proximité sont également réelles et concrètes. Ainsi, lorsqu'un commandant de brigade ou un commissaire de police exerce sur un territoire comportant une emprise sensible, des contacts directs sont établis. Dès lors qu'une plainte est déposée et qu'elle concerne directement ou indirectement une emprise sensible, des directives imposent

d'informer immédiatement le responsable de l'entité concernée, comme le commandant de base.

Dans une logique d'amélioration continue, nous avons toutefois identifié certaines lacunes et engagé des réflexions pour y remédier. Il est envisagé de faire évoluer nos outils afin d'accompagner davantage les agents en première ligne. Ceux-ci pourraient par exemple être utilement guidés par des questions systématiques permettant de détecter des situations sensibles et de déclencher automatiquement des alertes, lorsque cela est nécessaire.

Par ailleurs, l'anticipation repose largement sur la qualité du renseignement et la fluidité des échanges d'informations entre services. Cette dynamique collective constitue un atout majeur : les informations sont partagées, car chacun est conscient que cette coopération est indispensable pour progresser et limiter efficacement l'impact des attaques adverses.

M. le président Jean-Michel Jacques. Je vous remercie.

La séance est levée à douze heures quarante et un.

*

* *

Membres présents ou excusés

Présents. - Mme Valérie Bazin-Malgras, Mme Anne-Laure Blin, Mme Caroline Colombier, M. François Cormier-Bouligeon, M. Michel Criaud, Mme Geneviève Darrieussecq, Mme Sophie Errante, M. Damien Girard, M. José Gonzalez, M. David Habib, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Didier Lemaire, Mme Murielle Lepvraud, Mme Lise Magnier, M. Sylvain Maillard, M. Karl Olive, Mme Anna Pic, Mme Josy Poueyto, M. Alexandre Sabatou, M. Arnaud Saint-Martin, M. Aurélien Saintoul, Mme Sabine Thillaye, Mme Corinne Vignon

Excusés. - M. Christophe Blanchet, M. Frédéric Boccaletti, M. Manuel Bompard, Mme Cyrielle Chatelain, M. Moerani Frébault, M. Thomas Gassilloud, M. Daniel Grenon, Mme Catherine Hervieu, M. Bastien Lachaud, M. Abdelkader Lahmar, Mme Nadine Lechon, Mme Michèle Martinez, Mme Alexandra Martin (Alpes-Maritimes), Mme Natalia Pouzyreff, Mme Isabelle Rauch, Mme Mereana Reid Arbelot, Mme Marie-Pierre Rixain, M. Sébastien Saint-Pasteur, Mme Isabelle Santiago, M. Mikaele Seo, M. Boris Vallaud, M. Laurent Wauquiez

Assistait également à la réunion. - M. Christophe Naegelen