**M. le président Thomas Gassilloud.** Mes chers collègues, nous poursuivons notre cycle d'auditions sur les enseignements du conflit en Ukraine avec le général de division Aymeric Bonnemaison, chef du commandement de la cyberdéfense (Comcyber), placé sous l'autorité du chef d'état-major des armées.

Général, je vous remercie de votre présence parmi nous. Si votre nomination à cette fonction date du 1er septembre, votre intérêt pour le cyber est ancien. Vous avez notamment commandé le 54e régiment de transmissions, dit des *« traqueurs d'ondes »*, spécialisé dans l'écoute, la localisation et le brouillage des signaux de communication ennemis. Vous êtes co-auteur d'un livre publié dès 2013, intitulé *« Attention : Cyber ! Vers le combat cyber-électronique »*.

La Revue nationale stratégique (RNS) 2022 dresse ce diagnostic : *« Les États utilisent de plus en plus systématiquement l'arme cyber afin de défendre leurs intérêts stratégiques ou dans le cadre de tensions politiques »*. La guerre en Ukraine en est une remarquable illustration. Elle se déroule aussi dans le cyberespace, que votre ouvrage définit comme *« le maillage de l'ensemble des réseaux permettant une interconnexion informationnelle des êtres vivants et des machines »*.

Désormais, les cyberattaques visant des structures stratégiques et logistiques vont de pair avec les attaques plus conventionnelles, comme la Russie en a fait la démonstration en commençant l'agression de l'Ukraine, le 24 février dernier, par une attaque cyber visant le réseau satellitaire Viasat. Avant même l'éclatement du conflit, l'Ukraine était le théâtre d'une guerre hybride larvée, menée par la Russie, notamment dans le Donbass, mêlant manœuvres de guerre électronique et attaques informatiques, informationnelles et cognitives.

Mon général, vous qui êtes chargé de la lutte informatique offensive, défensive et d'influence, que retenez-vous de la cyberguerre que se mènent l'Ukraine et la Russie ? Quels enseignements en retirez-vous sur la conduite de la guerre en général et sur notre propre cybersécurité ?

Nous avons tous noté que l'objectif stratégique n° 4 de la RNS est spécifiquement consacré à *« une résilience cyber de premier rang »* et insiste sur la nécessité d'améliorer la résistance cyber de la France. Quelles sont les actions qui vous semblent prioritaires pour mieux adapter nos capacités ? Comment pouvons-nous contribuer à l'amélioration de la résilience des institutions européennes et internationales, et des partenaires de la France ?

**Général de division Aymeric Bonnemaison, commandant de la cyberdéfense.** Monsieur le président, mesdames et Messieurs les députés, je suis très honoré, à peine trois mois après avoir pris mes fonctions, de venir présenter mes analyses devant la représentation nationale. Je suis conscient des enjeux, en cette période charnière d'élaboration de la prochaine loi de programmation militaire (LPM) et surtout de fragilité stratégique, de versatilité géopolitique et d'expansion de la numérisation, dans notre société et dans nos armées, ce qui offre à la menace d'origine cyber l'opportunité de gagner encore en ampleur, en diversité et en sophistication.

Je suis responsable de la protection des systèmes d'information placés sous la responsabilité

du chef d'état-major des armées (Cema), ce qui inclut, dans les armées, les systèmes d'armes. Je suis responsable de la conduite de la défense des systèmes d'information du ministère des armées ainsi que de la conception, de la planification et de la conduite des opérations militaires de cyberdéfense, sous l'autorité du Cema.

Notre approche, assez singulière, couvre trois domaines de lutte : la lutte informatique défensive, qui occupe une majeure partie de mon commandement, la lutte informatique offensive et la lutte informatique d'influence (L2I).

En Ukraine, la cyberguerre a bel et bien eu lieu, contrairement à ce qu'a donné à croire l'absence de *« cyber Pearl Harbor »*. Des opérations de renseignement, d'entrave et d'influence ont d'ailleurs été menées dans le cyberespace au cours des dernières années.

La cyberconflictualité présente deux spécificités, qui faussent parfois l'analyse.

La première est un paradoxe des temporalités. La fulgurance des attaques, affranchies de la tyrannie de la distance, ne doit pas masquer leurs délais incompressibles de conception et de planification. Il faut des mois, voire des années pour construire une cyberattaque.

Contrairement à ce que l'on peut croire – je fais cet exercice de pédagogie depuis plusieurs années, y compris au sein du ministère – il ne s'agit pas d'un fusil cyber qui peut tirer sur toutes les cibles qui se présentent. Toute attaque cyber est taillée sur mesure, même si elle recourt à quelques outils et approches génériques. Elle suppose un travail préparatoire pour bien connaître sa cible, la caractériser et trouver le chemin pour la perturber, l'espionner, la saboter ou l'entraver.

Ensuite, le cyber a une faible lisibilité. Il est bien sûr assez difficile de se représenter le cyberespace, mais surtout, la guerre qui s'y mène est discrète, voire secrète. Cet aspect est masqué par l'exubérance des réseaux sociaux qui, en contraste, affirment beaucoup de choses plus ou moins étayées.

Ma présentation de notre analyse du conflit ukrainien ne débutera donc pas au 24 février dernier. Les opérations dans le cyberespace ont commencé bien avant le déclenchement des manœuvres dans les autres milieux, la terre, l'air et la mer. Elles ont exigé un haut niveau de préparation et d'anticipation.

Par ailleurs, mon analyse repose essentiellement sur des sources ouvertes, recoupées lors de mes discussions avec le chef du commandement cyber américain (USCYBERCOM) et les autres commandants cyber européens, qui commencent, par leurs échanges réguliers, à former une communauté.

L'étude de la période allant de 2014 au début de l'année 2022 permet de mettre en évidence la place de la guerre hybride dans la conception russe des conflits. Les Russes ont, de longue date, intégré à la manœuvre cyber et la manœuvre informationnelle, en liant fortement les deux dans leur action. Ils couvrent aussi bien le contenu que le contenant dans leur approche.

De 2014 à 2022, des attaques d'un très haut niveau technique ont visé des infrastructures

critiques en Ukraine, en commençant par des stations électriques en 2015. En 2016, une attaque bien plus complexe a visé un réseau électrique. Ces attaques sont les premières menées complètement à distance sur la fourniture d'électricité. La technique très sophistiquée mise en œuvre a suscité notre intérêt, dans la mesure où nous pourrions être amenés à la contrer. La première attaque a privé 225 000 personnes d'électricité pendant plusieurs heures. La seconde a réduit d'un cinquième la consommation de la capitale ukrainienne.

À partir de 2017, les attaques se sont diversifiées, prenant la forme d'une sorte de harcèlement et présentant une certaine viralité. Elles ont visé les réseaux ukrainiens publics et privés, et ont touché de grands groupes internationaux, tels que Saint-Gobain. Elles ont été associées à des opérations informationnelles, qui ont ajouté du commentaire aux coupures d'électricité pour exciter le mécontentement et saper la confiance de la population dans les institutions. Dans cette période, nous avons assisté à des opérations de subversion, notamment dans le Donbass, visant à la victimisation des russophones et à la surmédiatisation des grands programmes de construction russes, associées à une critique violente de l'incapacité des pouvoirs publics ukrainiens à préserver les réseaux électriques et les fonctionnalités essentielles à la vie courante.

Les Russes n'ont toutefois pas inscrit ces opérations dans le cadre de manœuvres tactiques, contrairement à leur pratique déjà ancienne : tel était le cas en Estonie en 2007, et en 2008, en Géorgie, où les opérations terrestres étaient très bien combinées avec les attaques informatiques.

Par ailleurs, à partir de 2014, l'État ukrainien a évolué dans son approche du cyber et entrepris des travaux majeurs pour se réformer en profondeur dans le cyberespace, notamment en travaillant sur le pilier stratégique. Début 2016, le gouvernement ukrainien a dévoilé sa première stratégie de cyberdéfense. Sur le plan capacitaire, le Parlement a simultanément alloué un budget pour la cyberdéfense et la protection des systèmes électoraux.

Une agence à compétence nationale, le Centre national de cybersécurité, comparable à notre Agence nationale de la sécurité des systèmes d'information (Anssi), a été fondée. Elle s'appuie sur des capacités opérationnelles de réponse aux incidents partagées par tous les pays ayant une expertise en cyberdéfense, et a ultérieurement développé une capacité dans le domaine privé. Sur le plan normatif, le gouvernement ukrainien a promulgué, à l'été 2017, une loi relative à la cybersécurité qui élargit les pouvoirs d'enquête et d'interception des services ukrainiens et crée une cyberpolice.

L'Ukraine a bénéficié d'un appui occidental précoce dans le cyberespace. Elle a travaillé sur ses vulnérabilités avec les cyberpuissances occidentales, au premier rang desquelles les États-Unis. Cet appui s'est avéré décisif pour la résilience de l'Ukraine dans les domaines des télécommunications et du numérique. Il repose sur un dialogue et des échanges accrus, ainsi que sur un rapprochement des normes et des procédures ukrainiennes avec les modèles occidentaux. L'Ukraine a ouvert une plateforme d'échange de données cyber qui est aux normes de l'Otan et de l'Union européenne (UE) et qui permet de partager rapidement les indices d'attaque et les premiers outils techniques permettant de s'en protéger.

Par ailleurs, plusieurs États, souvent limitrophes, ont proposé à l'Ukraine des solutions

numériques renforçant sa résilience, telles que l'hébergement redondant des données et des services numériques dans des centres de données situés notamment en Pologne et au Pays-Bas. Les États-Unis se sont investis directement et massivement, par le biais d'un soutien de l'État et d'acteurs privés tels que Microsoft et Google. Les compagnies privées numériques américaines ont fourni des solutions numériques de cybersécurité à l'Ukraine de manière continue et de plus en plus intense, au rythme de l'évolution des tensions avec la Russie.

L'implication directe des États-Unis s'est nettement intensifiée fin 2021. Tandis que les responsables des services de renseignement occidentaux observaient les préparatifs militaires russes et craignaient de plus en plus qu'une invasion s'accompagne d'une nouvelle vague de cyberattaques, le USCYBERCOM a déployé sur place une équipe d'experts militaires, chargée de découvrir si des attaquants russes avaient d'ores et déjà infiltré les systèmes ukrainiens.

Le plus souvent, les attaques cyber appliquent une stratégie de prépositionnement, laquelle exige un important travail préalable de renseignement, ce qui explique la complexité que j'évoquais. Toutefois, l'attaque n'est pas nécessairement menée dès qu'elle est techniquement réalisable : l'attaquant peut rester positionné et attendre son heure – en veillant toutefois à agir avant une mise à jour qui peut lui faire perdre son accès ; il faut trouver la combinaison adéquate pour frapper au bon moment.

L'arrivée des Américains chargés de détecter d'éventuels logiciels prépositionnés a été capitale au cours des semaines précédant le conflit. En deux semaines, leur mission est devenue l'un des plus grands déploiements du Cyber Command américain, mobilisant plus de quarante personnes des services armés américains. Ils étaient aux premières loges lorsque la Russie a intensifié ses opérations dans le cyberespace, en janvier, éprouvant les systèmes ukrainiens de façon inédite. Ces équipes se sont engagées dans une mission de hunting forward, qui consiste à arpenter les réseaux informatiques des partenaires à la recherche de signes de prépositionnement.

À la veille du 24 février donc, la Russie jouit d'une capacité cyber mature et éprouvée dans tous les domaines de lutte, qu'elle soit informationnelle ou offensive, et a entamé une opération de sape dans le cyberespace en combinant attaques informatiques et attaques informationnelles ; l'Ukraine, elle, dans cette première confrontation, a construit, ce qui sera essentiel pour la suite, des partenariats très structurants et une première capacité de cyberdéfense solide, ancrée à l'Occident et susceptible de bénéficier d'appuis importants.

J'en viens aux mois de février et mars 2022. Dans les premières semaines du conflit, les attaques informatiques russes visent les réseaux ukrainiens, qui ne sont pas uniformes. De façon générale, la cyberdéfense suppose de cartographier ses propres réseaux, ce qui n'est pas simple car les systèmes d'information ont été constitués le plus souvent au fur et à mesure, par une superposition de systèmes *ad hoc*. Nous n'avons pas toujours une vision globale de nos systèmes. En Ukraine, il faut distinguer les territoires du Donbass et de la Crimée, assez isolés et surtout très connectés aux réseaux russes, de l'ouest du pays, qui est fortement intégré à la fois à la Russie et au monde occidental.

Les attaques russes consistent surtout en opérations de déni de service, qui empêchent d'utiliser la téléphonie et d'accéder à certains sites internet, notamment ceux du

gouvernement, couplées à des coupures physiques, moins souvent évoquées.

Le cyberespace est organisé en trois couches. La première, la couche physique, rassemble les ordinateurs, les réseaux, les fils, les antennes. La deuxième, la couche logicielle, rassemble les dispositifs de codage, de protocole et de programmation qu'utilisent les machines. La troisième, la couche sémantique, particulièrement visible sur les réseaux sociaux, est constituée des éléments discursifs et informationnels. Par des actions de guerre classique, les Russes ont neutralisé des câbles et des points d'accès 3G et 4G, mais avec une certaine réserve et dans certains endroits seulement, car ils prévoyaient une guerre courte et pensaient réutiliser les infrastructures à leur profit.

Les effets de cette action ont été rapidement atténués par la distribution, au début du mois de mars, de routeurs de la société Starlink, qui ont permis aux populations, aux journalistes et aux autorités locales de maintenir un lien de communication minimal, et à nous-mêmes d'avoir des images de ce qui se passait. Le déploiement, dans des délais très brefs, de ce système de communication par satellite illustre les capacités et la réactivité de certains acteurs privés, en l'espèce Elon Musk, dans le contexte du *NewSpace*.

Dès les premières heures du conflit, les attaques cyber ont visé les ministères ukrainiens, selon un modèle appliqué en Géorgie. Il s'agissait d'empêcher les organes de gouvernement de dialoguer entre eux, voire d'empêcher le président ukrainien de dialoguer avec l'extérieur.

La deuxième vague d'attaques très poussées a visé les routeurs de communication par satellite KA-SAT, et donc la chaîne Viasat, qui est très utilisée par les troupes ukrainiennes. Starlink a en partie remédié à cette situation. La troisième vague d'attaques a plus largement visé les entreprises privées pour désorganiser le fonctionnement de la société ukrainienne.

Au cours des deux premiers mois de conflit, 350 attaques cyber ont été recensées, dont 40 % visant des infrastructures critiques susceptibles d'être utilisées par le gouvernement, l'armée, l'économie et la population, et 30 % des incidents ont touché les organisations gouvernementales ukrainiennes à l'échelon national d'abord, puis régional et municipal.

S'agissant des attaques informationnelles, nous avons assisté à une guerre inédite. Les forces en présence, rompues aux techniques de la guerre de l'information, ont saisi les opportunités offertes par le cyberespace dès les prémices du conflit. L'utilisation des réseaux sociaux, en particulier, a permis de rendre la guerre en Ukraine omniprésente dans l'opinion publique, ce à quoi nous avons tous assisté. Dès les premiers jours de la guerre, plus de 315 millions d'acteurs étaient engagés dans cette lutte informationnelle, jouant le rôle de relais d'informations.

On connaissait la domination russe dans le champ de la guerre informationnelle, mais elle a été contestée par les Ukrainiens. Les deux gouvernements ont adopté des stratégies de communication officielle diamétralement opposées dans leur forme.

La Russie s'est engagée dans un repli sur elle-même, en tentant de mettre sous cloche la sphère informationnelle et les contenus en réseau, en installant une sorte de rideau de fer numérique, en prenant un contrôle quasi total de l'information et en isolant progressivement

sa population du reste du monde. L'encerclement cognitif opéré par le Kremlin a progressivement stoppé la circulation des flux d'informations de la Russie vers le reste du monde et réciproquement.

Sur le plan des infrastructures informationnelles et sémantiques, la Russie jouit, dans le cyberespace, de sa propre couche sémantique et cognitive. Elle dispose d'un web russe quasi souverain, le Runet, qui capte la majorité des usages au sein d'un écosystème informationnel composé de réseaux sociaux, tels que VKontakte et Odnoklassniki, d'une messagerie, Mail.ru, et d'un moteur de recherche, Yandex. Cette évolution, entamée il y a une dizaine d'années, n'a pas abouti à un isolement complet, comme la Chine en a la capacité, mais à la création de réseaux sociaux et de services de messagerie propres, pour résister un peu à la pression des Gafam.

Les messages circulant sur ces réseaux visent à légitimer l'opération spéciale en déshumanisant les Ukrainiens et leur président, et en présentant la Russie ainsi que la population ukrainienne russophone comme menacées. Simultanément, ils déploient un discours destiné à l'opinion publique internationale en manipulant l'information, ce qui, à défaut de persuader, sème la confusion. Sur ce point, notre analyse est parfois biaisée : si, dans le monde occidental, tout le monde attribue la victoire dans la guerre informationnelle à Volodymyr Zelensky, tel n'est pas toujours le cas dans le reste du monde, où la lecture occidentale du conflit ne fait pas l'unanimité.

Le président ukrainien, quant à lui, a adopté une stratégie d'ouverture, communiquant massivement vers sa population et surtout vers l'Occident, en utilisant abondamment son image sur les réseaux sociaux et en déployant un narratif fin, systématiquement adapté à sa cible, qu'il s'adresse aux gouvernements étrangers, à l'UE, aux États-Unis ou à ses compatriotes, dans une démarche de président combattant parlant en tenue de soldat.

Les opinions publiques européennes ont rapidement pris fait et cause pour l'Ukraine. La diaspora ukrainienne en Occident relaie spontanément cette communication. Les responsables politiques ukrainiens ont transformé la guerre informationnelle officielle en guerre de l'émotion, par le biais des réseaux sociaux, en utilisant parfaitement Twitter, Instagram et TikTok en premier lieu.

Dans le cadre de cette stratégie d'ouverture, pour l'Ukraine, ou de fermeture pour la Russie, au-delà de la véracité ou non des informations, il est intéressant de noter que chaque camp diffuse un récit particulier de sa réalité, un narratif qui lui est propre, sans que jamais ces bulles informationnelles ne se rencontrent ni se confrontent. Chacun développe son propre public.

J'en viens aux caractéristiques du conflit dont nous pouvons tirer des leçons.

Nous, militaires, tendons à attribuer à la cyberguerre un rôle majeur dans les conflits du futur. Or, dans ce conflit-là, le cyber n'a pas tout fait, malgré la domination russe initiale. Quand la poudre parle, la lutte informatique offensive trouve ses limites. Dans la phase préparatoire de la guerre comme dans sa phase intensive, les actions de sabotage cyber ont été atténuées au profit d'une guerre classique bien plus létale, cinétique et brutale. On peut être tenté de

développer une vision un peu romantique selon laquelle tout se fera à l'avenir dans le monde virtuel, mais la réalité est qu'il est nécessaire de prendre en compte tous les aspects d'un conflit.

Là où le cyber joue un rôle particulièrement important, c'est avant le conflit, grâce au renseignement qu'il permet d'obtenir et à la possibilité qu'il offre de façonner les esprits, et aussi après le conflit, car la compétition, la contestation et l'affrontement demeurent en permanence dans le cyberespace.

L'armée informatique d'Ukraine, l'*IT Army*, qui a suscité de nombreux commentaires sur les réseaux sociaux, a eu une efficacité assez modeste. Elle a permis de structurer dans l'urgence de fortes capacités d'agression virales contre les Russes, mais les attaques menées ont été très désordonnées et d'un niveau technique relativement faible.

D'un point de vue plus strictement militaire, nous avons pris note de la difficulté qu'ont eue les Russes à intégrer pleinement les capacités cyber dans la manœuvre tactique, alors même qu'ils y étaient parvenus en Géorgie, en détruisant par voie navale, terrestre ou aérienne les stations de transmission de base, ce qui empêche l'ennemi de donner l'alerte ou de coordonner les moyens de secours. Certains y voient la conséquence de la relative impréparation du conflit, due à la croyance que la victoire serait rapide et aussi au secret qui a longtemps entouré son déclenchement, y compris parmi les gens en position de commandement, qui n'étaient pas tous informés de l'intention exacte du président Poutine.

Le deuxième enseignement de ce conflit est la capacité de la défense à prendre le dessus sur l'offensive, ce dont nous doutions. L'offensive, quand elle a le temps, cherche le maillon faible et le trouve. Toute chaîne de moyens connectés en a un, qu'il soit humain ou logiciel, ce qui permet d'y faire intrusion. Grâce à une défense en profondeur, assurée par les capacités ukrainiennes renforcées par les capacités américaines et avec l'apport significatif des Gafam, notamment de Microsoft s'agissant des analyses, l'offensive a été bien moins percutante et efficace que prévu.

Cet avantage par le défensif constitue un véritable changement de paradigme pour les divers commandements cyber et nous rend un peu espoir – nous protégeons nos réseaux en permanence en ayant parfois le sentiment d'édifier une ligne Maginot, dont chacun sait ce qu'elle a donné. Il faut des défenses permettant de protéger nativement nos réseaux, associées à une capacité de patrouille sur nos réseaux et de vérification incessante.

Je ne m'attarderai pas sur la politique américaine de hunting forward, sinon pour dire qu'elle est relativement agressive, car elle ouvre aux Américains les réseaux des pays qui font appel à eux. En l'occurrence, elle a beaucoup aidé l'Ukraine, mais cette démarche va assez loin. En pratiquant une forme d'entrisme sur les réseaux concernés, elle les protège, mais avec une présence marquée au service de la diplomatie, ce dont le général Nakasone ne se cache pas. Son appui est une forme de réassurance donnée à plusieurs pays d'Europe de l'Est.

Le troisième enseignement du conflit est la faible lisibilité non seulement des actions, mais aussi des acteurs.

Les « *hacktivistes* » se mobilisent en fonction de leurs opinions, avec d'importantes capacités et une bonne maîtrise technique. Leur coordination, en revanche, est malaisée, et les effets de leur action un peu désordonnés. Hormis une forme de harcèlement, leur action n'a pas été d'une grande efficacité.

Des groupes cybercriminels ont mené des attaques pour le compte de certains services de renseignement, dans le cadre d'une porosité accrue entre ces deux mondes, ce qui complique l'attribution des attaques informatiques. Les modes d'action utilisés par les cybercriminels sont parfois détournés par des services étatiques, et certains cybercriminels sont parfois mandatés par eux pour conduire des opérations.

Il règne dans le cyberespace une grande confusion entre les divers acteurs. Ma génération, qui a connu les guerres asymétriques, sait que la distinction entre civils et militaires n'a rien d'évident, mais elle encore plus complexe dans le cyberespace.

Quant aux Gafam, ils ont pris une importance considérable dans cette affaire. Certes, ils ont largement contribué à la protection de l'Ukraine, mais en prenant un poids qui soulève des questions d'ordre politique.

**M. le président Thomas Gassilloud.** Merci pour cette intervention complète et aussi équilibrée, car elle démontre l'importance du champ cyber dans la manœuvre globale tout en rappelant qu'il ne fait pas tout.

Par ailleurs, l'irruption d'acteurs privés, tels que les Gafam ou Starlink, qui jouent un rôle désormais considérable dans l'évolution du monde, soulève des questions sur leur articulation et sur la réaction des États.

Nous en venons aux interventions des orateurs des groupes.

**M. Mounir Belhamiti (RE).** Dès l'invasion de la Crimée, le conflit ukrainien a été source d'enseignements dans le domaine cyber. Auparavant, la Russie avait déjà affiché sa force de frappe cyber lors d'interventions dans plusieurs pays, dont les États-Unis, le Sénégal, le Mali et la France. Cette puissance est notamment due à une politique permissive vis-à-vis des pirates informatiques russes qui, depuis la fin de la guerre froide, doivent travailler aussi pour les services russes s'ils veulent maintenir leurs activités crapuleuses sans être inquiétés. Cet hébergement d'activités cybercriminelles est une particularité russe.

En 2014, la Russie a tenté d'influer sur l'élection présidentielle ukrainienne en lançant des attaques par déni de service sur des sites gouvernementaux. En les rendant inaccessible ou en les effaçant, Moscou voulait démontrer sa capacité à faire un coup de force et amener les Ukrainiens à choisir un président pro-russe pour éviter des représailles.

Dans la semaine précédant l'invasion russe, l'Ukraine a dénombré plus de 200 cyberattaques sur son territoire, visant des sites gouvernementaux, des hôpitaux et des moyens de production. Par le biais de ce *black-out*, la Russie espérait faciliter son intervention.

Le 26 février 2022, le vice-premier ministre ukrainien, ministre de la transformation numérique,

M. Fedorov, a proposé à toute personne sachant pirater des réseaux et souhaitant aider l'Ukraine de se manifester en attaquant la Russie. Il en est résulté une riposte d'ampleur : de nombreux hackers ont soutenu l'Ukraine, aux côtés de grandes sociétés que vous avez citées. Chaque jour, nous mesurons l'impact de la contre-attaque ukrainienne, qui se manifeste en faisant tomber des sites pro-russes ou en révélant des positions russes grâce aux flux vidéo ou aux signaux GPS.

Cette cyber-riposte n'est cependant pas, comme vous l'avez dit, susceptible d'inverser le cours des choses. L'un des enseignements que nous pouvons tirer de cette guerre est notre vulnérabilité face à des pirates informatiques, qui pourrait se traduire par une mise en déroute de nos propres outils de production. Chaque appareil électronique est une surface d'attaque potentielle et, bien que des moyens soient mis en œuvre depuis cinq ans dans un cadre militaire, nous constatons que l'obsolescence de nos défenses est très rapide et que l'adaptation qui est possible dans un cadre militaire est parfois plus difficile à réaliser et à suivre dans un contexte civil, notamment au niveau des entreprises et des collectivités.

Il devient donc nécessaire de penser en termes d'interopérabilité entre défense cyber militaire et défense cyber civile. Je rappelle que, le 4 décembre dernier, l'hôpital de Versailles a été victime d'une cyberattaque majeure, pouvant nuire à la prise en charge de patients et même conduire au décès de certains d'entre eux.

Pensez-vous qu'à l'heure du post-quantique, nous ayons les moyens de faire face à un tel niveau de menace ? Selon vous, comment augmenter efficacement le niveau de cybersécurité du pays pour nos points vitaux tant civils que militaires ? Enfin, quelles sont les priorités auxquelles devra répondre la future LPM ?

**M. José Gonzalez (RN).** Presque un an s'est écoulé depuis le début du conflit qui oppose la Russie à l'Ukraine, ou, pour être précis, depuis le début de l'agression de l'Ukraine par la Russie, et nous avons aujourd'hui des éléments pour comprendre et étudier la cyberguerre qui oppose les deux pays et, plus encore, les répercussions qu'elle peut avoir en Europe.

Bien moins évidente que le conflit qui se joue directement sur le champ de bataille, la guerre menée dans le cyber s'est très vite révélée moins alarmante que ne le redoutaient les différents observateurs occidentaux. C'est d'ailleurs là – peut-être le confirmerez-vous – l'un des enseignements les plus surprenants de ce conflit. En effet, si l'on s'attendait à de multiples cyberattaques à l'encontre de l'activité économique et à une volonté de paralyser certains États, force est de constater qu'aucune offensive de grande ampleur n'est à déplorer à ce jour. Cela est d'autant plus déroutant qu'on sait comment la Russie s'est illustrée dans le domaine cyber, d'un point de vue tant technique qu'économique et social. Il est donc légitime de s'attendre à de féroces hostilités de sa part à l'encontre de ses adversaires, et c'est le comportement qu'elle manifestait avant que le conflit ne prenne officiellement forme. On se souvient notamment des vols de données bancaires, militaires ou relatives à des personnalités diplomatiques ukrainiennes et autres attaques numériques observées quelques jours avant que la guerre ne commence.

Dans ces conditions, est-il légitime de parler de cyberguerre intense et massive ? Cela ne dissimule-t-il pas une forme d'attaque plus subtile et discrète ? Dans une telle perspective,

comment les pays qui ne sont pas directement belligérants interviennent-ils – vous avez déjà abordé ce point en évoquant l'intervention des Américains ?

**M. Aurélien Saintoul (LFI-NUPES).** Vous avez mis l'accent sur la dimension d'influence que revêt l'action cyber des Russes et sur l'enjeu qu'il y a à être capable de façonner préalablement l'opinion. On voit surgir là un risque pour le pluralisme. L'influence fait partie des priorités de la revue nationale stratégique. Comment appréciez-vous le risque que cela peut faire peser sur nos principes démocratiques et la façon dont nous pouvons agir dans le domaine de l'influence sans nous contredire ?

Vous avez, par ailleurs, souligné que la nature même des actions cyber exige une longue préparation et un important temps de latence. Comment envisagez-vous l'amélioration de l'articulation de vos services avec ceux du renseignement ? Un optimum est-il atteint ou une amélioration est-elle possible ?

Du point de vue de la conduite des opérations, s'agissant de l'Ukraine mais pas seulement, que peut nous apprendre l'action cyber quant aux intentions d'une puissance belligérante ? Nous voue-t-elle au brouillard ou, au contraire, apporte-t-elle une information qui peut nous éclairer quant aux buts de guerre réellement poursuivis ? Cette question est particulièrement importante dans le conflit actuel, étant donné son degré d'imprévisibilité ou d'irrationalité, qui a frappé tous les observateurs.

Vous avez également évoqué le rôle des entreprises ou d'infrastructures comme *Runet* ou *VKontakte*, et la façon dont les Russes ont constitué des infrastructures propres. De tels objectifs peuvent-ils participer à une stratégie de résilience pertinente pour un pays comme la France ?

Enfin, où en sommes-nous dans le domaine quantique et comment concevez-vous l'évolution de la menace dans ce domaine ?

**M. Jean-Louis Thiériot (LR).** Dans la guerre cyber qui se déroule aujourd'hui en Ukraine, y a-t-il eu, et à quel niveau, des attaques cyber dans les pays de la ligne de front, c'est-à-dire ceux, des pays baltes jusqu'à la Roumanie, qui se trouvent en première ligne ? Quels liens avez-vous pu observer et quel est l'état de la situation ?

En deuxième lieu, vous avez évoqué le lien entre guerre cyber et guerre informationnelle. S'il est très clair qu'à ce stade, l'Ukraine a probablement gagné la partie de la guerre informationnelle en Occident, la situation n'est pas du tout la même dans le reste du monde, où les perceptions sont très différentes. Comment expliquez-vous cette différence et pourquoi une communication ouverte à l'ukrainienne fonctionne-t-elle très bien en Occident et moins bien ailleurs ? Il serait, pour nos stratégies futures, très important de le comprendre.

En troisième lieu, l'Ukraine mène-t-elle aussi – pour autant qu'on puisse le savoir, ou que vous puissiez nous le dire – des opérations cyber offensives sur le territoire russe et en direction des infrastructures russes, et avec quel résultat ?

Vous évoquiez, enfin, la question majeure de l'attribution des attaques. Il y a des attaques

informatiques sur tout le territoire national : Mounir Belhamiti a très justement rappelé l'attaque subie par l'hôpital André Mignot de Versailles et mon département de Seine-et-Marne a été victime, comme sept autres, d'attaques informatiques majeures dont l'attribution est difficile, même si de sérieux doutes nous orientent vers l'est. Que pouvez-vous donc nous dire à propos de l'attribution, qui est aussi une question politique ?

Question corollaire : quel rôle jouent les proxys, dont on connaît l'importance en Russie et en Ukraine ? La France devrait-elle réfléchir elle aussi à l'utilisation de proxys, afin de mener des actions discrètes ?

**M. Fabien Lainé (Dem).** La situation en Ukraine doit nous inspirer pour tout ce qui concerne l'endommagement de nos infrastructures d'importance critique, la perturbation du fonctionnement de nos services publics, le vol de renseignements soumis à la propriété intellectuelle ou les entraves visant nos activités. Pendant la crise du covid-19, nous avons tous étés marqués, notamment dans les Landes, par la longue et douloureuse attaque de l'hôpital de Dax, qui a été l'une des premières de cette nature et qui a placé les personnels et plus encore les patients dans une situation critique.

Nous pouvons redouter des attaques visant nos opérateurs d'importance vitale à l'occasion des grands événements qui se profilent, comme la Coupe du monde de rugby ou les Jeux olympiques. Au-delà de la souveraineté nationale, on voit aussi les effets de la guerre informationnelle par exemple au Mali, qui a beaucoup animé les débats dans cette enceinte durant le précédent mandat. À l'Assemblée parlementaire de l'Otan, d'où plusieurs collègues et moi-même revenons, on débat du concept stratégique adopté en 2022, notamment à l'égard de la Fédération de Russie, considérée comme un compétiteur qui teste notre résilience et tente d'abuser de l'ouverture de notre interconnexion. Ce sont là pour nous des interrogations.

Vous savez que nous travaillons sur la prochaine loi de programmation militaire. Quels sont, à cet égard, vos attentes, vos conseils et vos propositions, qui seraient fort utiles pour nos travaux ?

**Mme Anne Le Hénanff (HOR).** Compte tenu de la position ferme de la France vis-à-vis de la guerre en Ukraine, l'invasion dormante par la Russie – ce que vous appelez la guerre discrète – a-t-elle commencé en direction de l'Europe, et en particulier de la France ? Nos réseaux ont-ils commencé à être envahis par les invasions cyber dormantes ? Ce n'est pas de la science-fiction.

Vous avez également relativisé l'impact des cyberguerres et rappelé le rôle déterminant des guerres traditionnelles dans l'issue des conflits, laissant entendre que les États bien dotés et bien préparés l'emporteront sur ceux qui manient l'outil cyber. Ne croyez-vous pas cependant à une guerre 100 % cyber dans un avenir proche ? Faut-il systématiquement la lier à la guerre traditionnelle ?

Lors de l'audition du chef d'état-major des armées, j'avais souligné un cloisonnement, volontaire ou involontaire, entre la stratégie du ministère des armées en matière de cyberdéfense, assez secrète pour le commun des mortels – les Français n'ont pas connaissance

des travaux de recherche ni des analyses sur l'attaque de demain – et celle des autres ministères qui traitent de ces questions, comme le ministère de l'intérieur ou les ministères chargés du numérique ou des collectivités locales. Une certaine ouverture du ministère des armées vers la société civile, notamment vers les collectivités locales, qui devront tôt ou tard faire face à la cyberattaque majeure, est-elle envisageable ? Ce jour-là, ce ne sera pas un hôpital, mais tout le territoire qui sera visé. Un décloisonnement, un accompagnement à la gestion de crise et à l'anticipation sont-ils envisageables pour éviter cette situation ?

**M. le président Thomas Gassilloud.** Pouvez-vous également nous indiquer quels sont les rôles respectifs de l'armée et de l'Anssi, qui est un acteur important, afin que nous ayons un bon aperçu de la cohérence globale de notre stratégie ?

**Général de division Aymeric Bonnemaison.** Je commencerai par l'Anssi. La France a choisi de faire d'une agence nationale l'autorité et l'acteur central dans le domaine de la cybersécurité. L'Anssi ne pouvant cependant porter seule le poids de ce lourd écosystème, une structure dénommée C4, ou Centre de coordination des crises cyber, a été créée afin de permettre des échanges très rapides. J'y participe pour ma part une fois par mois mais nos équipes se rencontrent plus régulièrement et nous disposons même maintenant d'une partie dénommée C4 permanent. Dès qu'une attaque cyber est signalée, les échanges se tiennent très rapidement pour assurer un large partage des analyses au sein de l'État. Y prennent part le Secrétariat général de la défense et de la sécurité nationale, qui préside ces échanges, l'Anssi, différents services de renseignements comme le Comcyber, la DGA-MI (Direction générale de l'armement Maîtrise de l'information), qui a une expertise dans ce domaine, et le ministère des affaires étrangères. C'est dans cette enceinte que nous abordons bon nombre des sujets que vous avez évoqués.

L'attribution d'une attaque est très complexe. Tout d'abord, si je peux vous dire combien d'attaques j'ai détecté, je ne peux pas vous dire combien j'en ai subi. Il se peut que des prépositionnements aient été effectués sur nos réseaux ou dans nos entreprises, avec des opérations de sabotage ou, surtout, de récupération de données et d'espionnage. La démarche chinoise, par exemple, se veut très discrète afin de piller notre savoir. Les Russes, quant à eux, pratiquent plutôt une guerre informationnelle et des actions d'entrave, ce qui n'exclut pas pour autant des opérations de renseignement préalables.

Nos services assurent la détection pour les réseaux du ministère, et l'Anssi dispose de nombreux relais dans l'État. Les services de renseignement nous aident à caractériser l'attaque en menant une étude technique fine basée sur des moyens dont nous ne disposons pas au sein de l'état-major des armées. Les services de renseignement creusent la question et mettent à profit leur première analyse, dont ils tirent des éléments techniques de caractérisation qui permettront de déterminer un mode d'action adverse.

Cependant, pour mener une attaque, il n'y a rien de mieux que de se cacher derrière un profil-type d'attaque auquel recourent les cybercriminels, et d'employer les outils du *dark web* qu'ils utilisent. À partir des éléments dont nous disposons, qu'ils soient techniques ou concernent le mode d'action, il est très difficile d'être certain de l'imputation technique d'une attaque. Certains éléments permettent néanmoins de le faire et, fort heureusement, les attaquants commettent aussi des erreurs.

Une fois l'imputation technique acquise, vient l'attribution, qui a un caractère plus politique et qui échappe au niveau où nous intervenons : il s'agit de décider politiquement, au nom de la France seule ou en coalition, si l'attaque sera attribuée à un pays déterminé. Ce processus est assez bien structuré dans l'État.

Pour ce qui est des collectivités territoriales, la tâche est importante. Lorsqu'on me parle de l'interopérabilité permanente et de l'interconnexion de l'armée de demain, je ne manque jamais de répondre que l'interopérabilité, si elle nous rend plus efficaces dans l'action militaire, nous rend aussi plus vulnérables sur le plan cyber. Chaque interconnexion crée une faiblesse. Il y a là un vrai défi.

Pour ce qui concerne les collectivités territoriales, ce défi ne relève pas seulement du ministère des armées. Nous y travaillons en nous efforçant d'être plus présents dans les lycées et auprès des jeunes, mais il faut sensibiliser la population avec des formations très en amont. En effet, des mesures simples peuvent permettre d'éviter une contamination trop rapide ou de détecter certains éléments.

Il ne faut pas non plus oublier nos entreprises et leurs sous-traitants, qui doivent monter en gamme sur le plan cyber. En effet, certaines entreprises nous disent encore qu'elles ne risquent rien parce qu'elles n'intéressent personne ! Il y a dix ans, lorsque nous avons écrit notre livre, beaucoup nous jugeaient pessimistes sur ce point, et on me trouve peut-être un peu trop optimiste aujourd'hui.

À tous les niveaux de l'État, une acculturation est nécessaire, dont nous sommes tous responsables. Nous y contribuerons par le biais de la journée défense et citoyenneté, qui nous permet de sensibiliser les jeunes – et aussi, je ne vous le cache pas, d'essayer de les recruter. Nous intervenons également dans des lycées, où nous proposons des jeux et activités ludiques du type Capture the flag qui permettront de faire venir des jeunes vers les domaines techniques. Alors que de nombreux jeunes abandonnent aujourd'hui les mathématiques assez tôt, cela permet de leur en faire découvrir une autre utilité et une autre vision. On peut être passionné de géopolitique et codeur, on peut être passionné de langues sans être hermétique à la technologie. Il y a là quelque chose à construire avec l'éducation nationale – j'ai déjà rencontré le directeur général de l'enseignement scolaire à ce propos – en vue de créer une dynamique. La technique, les mathématiques, ce n'est pas quelque chose de sale. Nous devons parvenir à attirer des jeunes. Je rencontre aujourd'hui un déficit de personnel et j'ai besoin de recruter. Je parraine d'ailleurs une cadette de la cyberdéfense. On s'aperçoit en effet que les formations d'ingénieurs en France peuvent accueillir plus de monde et que les femmes y sont peu nombreuses, peut-être par autocensure. Or aucune raison ne justifie leur absence dans le cyber. Nous devons mener dans ce domaine un travail collectif.

Nous travaillons, bien évidemment, sur le post-quantique, qui nous rendra peut-être plus vulnérables mais également meilleurs : le fait de pouvoir croiser des données et détecter des signaux faibles beaucoup plus rapidement nous fait progresser, mais le quantique permettra également de générer de nouvelles formes d'attaques. Dans le monde de la cyberdéfense, on ne peut jamais s'arrêter, on n'a jamais trouvé la solution, que ce soit en attaque informationnelle ou sur les réseaux. L'outil que j'utilise aujourd'hui ne sera plus valable demain, parce que le mode d'action aura été repéré ; il doit, en outre, être adapté à chaque

cible. Mais ce qui est une difficulté pour l'attaquant est toujours bénéfique au défenseur. Autre aspect du travail dans le post-quantique, nous réclamons des financements en matière de chiffrement afin d'anticiper les techniques de demain, qui devront résister à ces outils. Les enjeux sont nombreux, mais nous y travaillons.

On m'a demandé si la cyberguerre était intense et massive, ou plutôt fine. Elle est, en réalité, un peu tout cela. Quant à savoir si on peut gagner une guerre par le cyber… Tout dépend de l'objectif, et notamment de la volonté de conquérir ou non du territoire. Ce qui est certain, c'est qu'on peut mettre à genoux un État : le Costa Rica s'est trouvé cet été en état d'urgence à la suite d'attaques sur tous ses réseaux. Il ne pouvait même plus payer ses fonctionnaires ni son armée. Le cyber peut servir à affaiblir durablement un État de façon sournoise et dans la durée, ou de façon brutale et visible. Mais, pour un militaire, même si le cyber permet de remporter des victoires, au même titre que les frappes aériennes par exemple, on ne gagne pas une guerre si on ne tient pas le terrain. Sans cyber nous sommes sûrs de perdre, mais nous ne gagnerons pas avec le cyber seul.

C'est là, du reste, l'un des défis de la LPM. Je ne peux pas trop m'avancer sur ce sujet : j'ai certes des exigences, mais c'est un gros édredon et je ne sais pas de quelle taille sera la valise, d'autant que toutes les armées sont aujourd'hui confrontées à une guerre de haute intensité. Le cyber s'ajoute aux autres milieux et ne se substitue pas à l'un ou l'autre d'entre eux. Même si des efforts sont faits, sans doute aurons-nous du mal à tout faire entrer dans la valise.

Pour ce qui est des risques pour la pluralité et pour la nation, je rappelle que je ne suis que l'un des acteurs de la lutte informatique d'influence, agissant pour les armées et en appui aux opérations militaires, dans un cadre très strict, qui respecte le droit international, le droit national, ainsi que des règles éthiques plus restrictives. Ainsi, je ne travaille pas sur le territoire national, mais en appui sur des théâtres d'opérations. Ce cadre est très contraint et une interaction se fait au niveau supérieur au mien avec les autres ministères pour porter les messages et assurer la coordination.

Les attaques que nous subissons dans la sphère de l'Afrique francophone montrent que nous avons encore bien du travail à réaliser ensemble, qui ne concerne pas seulement les armées mais de nombreux ministères. Ce ne sont pas les armées qui assurent la stabilité d'un pays, mais tous les acteurs ensemble, avec l'économie et la culture. C'est un travail commun que nous devons sans doute un peu mieux structurer – c'est en cours. Les points que vous évoquez ont été abordés notamment lors de la création de Viginum (service de vigilance et de protection contre les ingérences numériques étrangères) et nous disposons désormais d'un cadre assez strict, qui permet de faire les vérifications appropriées. Nous sommes, en tout cas, tous sensibilisés aux risques de dérives possibles en la matière, y compris dans les services de renseignement, où l'application de la loi est très contrôlée.

Pour ce qui est des attaques visant des pays frontaliers, il se trouve que, depuis la guerre d'Ukraine, mes échanges avec mes partenaires sont devenus plus simples. Le cyber a un petit côté régalien, surtout pour les aspects liés à l'offensif et l'influence, mais qui a moins de raisons d'être pour ce qui concerne le défensif. Aujourd'hui, le partage très rapide des informations dès que l'un d'entre nous est attaqué, dans le cadre otanien ou européen, assorti

d'une capacité d'intégrer les données techniques de la manière plus fluide possible, est au cœur de nos préoccupations. Les Américains l'ont déjà fait en publiant des attaques russes ; or lorsque vous publiez le type de virus et les données correspondantes, cela permet de le filtrer et de le trouver. Jusqu'à présent, les nations avaient plutôt tendance à garder ces informations par-devers elles, y compris pour les réutiliser ultérieurement, mais aujourd'hui la dynamique consiste plutôt à les publier au plus vite afin d'éviter que d'autres pays soient contaminés. Ainsi, de même qu'elle a réveillé l'Otan, l'attaque de Poutine a finalement accéléré le partage des données, que nous travaillerons à poursuivre dans les années prochaines.

Pour ce qui est des attaques visant les territoires, le ministère des armées n'est pas l'acteur central de la réponse au sein de l'État. En revanche, c'est l'un des ministères qui ont le plus travaillé et qui disposent d'une première maturité sur ces sujets. Nous sommes bien entendu susceptibles de renforcer l'Anssi si elle a besoin d'un appui particulier, comme nous l'avons déjà fait au Monténégro. Des acteurs privés interviennent aussi pour l'État dans cette remédiation, également labellisés par l'Anssi. Il arrive d'ailleurs qu'on nous reproche, nous acteurs publics, de concurrencer les acteurs privés sur un marché qui pourrait leur être ouvert.

Notre réflexion sur les crises majeures doit être intégrée dans la loi de programmation militaire, mais tout dépendra du niveau d'ambition que nous nous fixerons dans ce domaine. En tant que militaires, nous participons évidemment à la défense nationale, mais ce que nous avons développé dans le cadre des armées sert déjà à protéger nos systèmes – ce qui est déjà un défi. En cas d'intervention sur le territoire national face à une attaque majeure, cyber ou d'une autre nature, nous aurons aussi besoin de nous déployer. Nous le ferons notamment à l'occasion des Jeux olympiques, même si le dispositif relèvera avant tout du ministère de l'intérieur, et je serai pour ma part responsable de la protection cyber des unités déployées par les armées. Si donc nous devions avoir la mission d'être plus présents dans les territoires, ce serait une ambition de la LPM et nous devrions en avoir les moyens.

Cela soulève bien sûr la question de la réserve, qui n'est pas si facile à construire et à maintenir dans la durée. Étant désormais un peu ancien dans l'institution, j'ai connu des cas, notamment lorsque je commandais un régiment en Alsace, où l'on a créé une réserve, où l'on a fait des promesses, où des gens se sont engagés, notamment vis-à-vis de leurs entreprises, et où des coupes budgétaires ont tout mis par terre. Si donc nous entrons dans une dynamique de réserve, nous devons nous structurer pour l'accueillir, mais aussi assurer une continuité sur toute la durée de la formation militaire.

S'agissant des opérations offensives ukrainiennes qui pourraient être menées sur le territoire russe, sans doute y en a-t-il, mais j'avoue être assez peu informé sur cette question. Certaines opérations ont été conduites par les États-Unis, assumées notamment par le général Nakasone. Cependant, les Ukrainiens sont en plein conflit. Or, je vous l'ai dit, une attaque bien structurée en lutte informatique offensive n'est pas le fait d'un homme en capuche qui travaille seul dans une cave : c'est un vrai travail d'équipe, qui associe des compétences diverses et qui demande des conditions préalables et un tempo qui ne sont pas forcément ceux d'un pays submergé par une attaque et qui mène déjà une guerre classique. Des gens agissent certainement – je pense en particulier à l'IT Army – mais en ordre sans doute un peu dispersé.

Pour ce qui est des invasions dormantes, j'aimerais vous dire qu'il n'y a pas de risque, mais

nous ne le savons pas. Ce qui est certain, c'est que nous ne sommes pas le seul ennemi des Russes, qui eux aussi sont assez occupés en Ukraine. Certains de leurs outils ont été détectés lors des attaques qu'ils ont tentées dans ce pays et qui ont été révélées, ce qui nous donne un peu de lisibilité, mais le métier de Comcyber pousse à une grande prudence et à une grande humilité. Quand je ne détecte pas d'attaque, cela ne signifie pas qu'il n'y en a pas, mais seulement que je ne l'ai pas vue.

**M. le président Thomas Gassilloud.** Je reviens sur la question de M. Saintoul sur la stratégie russe en matière de résilience. À l'échelle du monde, certains États restent très ouverts, comme les pays d'Europe et les États-Unis d'Amérique, tandis que d'autres cherchent à mieux maîtriser leur internet. Les Chinois parviennent pratiquement à s'isoler et les Russes travaillent dans le même sens. Comment être résilients dans le domaine cyber lorsque toutes les portes sont ouvertes ? N'est-ce pas là notre difficulté majeure ? La stratégie de la Russie et de la Chine, qui consiste à mieux maîtriser leur réseau internet, tant pour des raisons de résilience nationale que pour contrôler les informations qui circulent, vous semble-t-elle pertinente ?

**Général de division Aymeric Bonnemaison.** Nous avions quelque peu anticipé cette fragmentation d'internet. Au vu des pays qui la pratiquent – la Chine, la Russie et l'Iran – c'est un signe peu encourageant d'un point de vue démocratique.

En matière de *data centers*, le développement d'une souveraineté française ou européenne est tout à fait opportun. Dans ce domaine, nous disposons en France d'une technologie qui monte et que nous devons soutenir. Ne soyons pas naïfs, y compris s'agissant de nos alliés, car ces derniers ont aussi des intérêts propres. Il faut aller vers plus de capacités intégrées en France.

Quant à la fermeture d'internet, c'est une question qui se pose aussi dans le milieu militaire. Comme je l'ai déjà dit, les armées veulent de plus en plus d'interopérabilité car c'est ainsi qu'elles gagneront – mais à condition que le COMCYBER parvienne à préserver la sécurité de cette interconnexion !

Vous m'avez enfin demandé pourquoi l'influence ukrainienne n'avait de succès qu'en Occident : c'est parce qu'elle y a trouvé un terreau favorable. Il existe des enjeux géopolitiques expliquant que certains pays ont intérêt à ne pas croire Volodymyr Zelensky, parce qu'ils subissent des pressions de la part de la Russie ou qu'ils ont des engagements ou des intérêts qui les dissuadent, quoi qu'il arrive, de pencher de l'autre côté. Enfin, les populations n'ont pas toutes le même niveau d'information ni d'éducation dans leur accès à l'information.

**M. le président Thomas Gassilloud.** Nous en venons aux questions individuelles.

**M. Jean-Michel Jacques (RE).** En décrivant la guerre d'influence et la guerre informationnelle actuelles, vous avez dit que chaque partie parlait à son propre public. Cela signifie-t-il qu'elle n'arrive pas à toucher le public adverse, et donc que la cyberdéfense est plus facile que la cyberattaque ? Cela influence-t-il notre doctrine ?

**Mme Michèle Martinez (RN).** Une enquête menée en 2021 par les services de la plateforme cybermalveillance.gouv.fr auprès des communes de moins de 3 500 habitants a révélé que 65 % d'entre elles estimaient que le risque numérique était faible, voire inexistant, ou disaient ne

pas savoir l'évaluer. Les cyberattaques menées dans le cadre de la guerre en Ukraine sont certes dirigées contre des services gouvernementaux, mais l'impréparation et les lacunes cruelles des collectivités locales, notamment des communes rurales et de taille moyenne, en matière de cybersécurité apparaissent quand même trop peu prises en compte. Si ces collectivités peuvent apparaître, au premier abord, comme des cibles non stratégiques, elles n'en disposent pas moins de nombreuses données sensibles, qui vont des registres de l'état civil aux marchés publics en passant par des dossiers complets d'administrés ou des documents électoraux. Le risque est grand. L'État a-t-il pris pleinement conscience de ce problème, qu'il ne pourra sans doute résoudre qu'en investissant fortement dans l'accompagnement des collectivités ?

**Mme Nathalie Serre (LR).** Vous avez évoqué le rôle important joué par les géants du numérique, les Gafam, qui ne sont pourtant pas des États mais des entreprises. Leur action est-elle positive, négative ou neutre dans la défense d'un pays ? Avons-nous intérêt à exercer sur eux un contrôle politique ou à développer nos propres réseaux ?

**M. Jean-Marie Fiévet (RE).** Depuis le mois de février, l'invasion de l'Ukraine par la Russie se déroule dans différents champs opérationnels : sur terre, en mer et dans les airs. Le conflit prend toutes les dimensions et occupe également, de manière moins médiatique, l'espace cyber. De nombreux assauts sont menés, mêlant attaques informatiques, tentatives de désinformation, destructions de réseaux et opérations d'espionnage. Si la Russie est l'une des menaces principales en matière de cyberattaques, l'armée ukrainienne fait aussi preuve de résilience. Vous avez rappelé que la Russie avait déjà conduit diverses cyberattaques à l'encontre de l'Ukraine avant l'invasion, mais ces actions sont désormais utilisées en complément des opérations militaires physiques.

Les cyberattaques russes ont aussi visé d'autres pays, notamment des États membres de l'Union européenne. Elles se font de plus en plus menaçantes et ciblent y compris les États les plus avancés en cyberdéfense. Cet accroissement de la menace a d'ailleurs entraîné un renforcement de la coopération internationale en la matière. Alors que la Commission européenne a présenté différents plans visant à renforcer la cybersécurité en Europe, pourquoi ne pas encourager davantage la coopération européenne, en créant par exemple une agence cyber au fonctionnement similaire à celui de l'agence Frontex, qui permettrait d'harmoniser les pratiques de cyberdéfense de l'ensemble des États membres ?

**M. Pierrick Berteloot (RN).** Nous pouvons tirer de nombreux enseignements du conflit russo-ukrainien. Qu'il s'agisse de l'utilisation de drones-suicide, du retour de la logique de masse des armées ou de l'usage d'une technologie militaire moins avancée, mais beaucoup plus facile et rentable à produire, nous avons la chance de pouvoir produire un retour d'expérience, que nous pourrons exploiter. L'un des volets en est le domaine du cyber, qui n'est plus à sous-estimer puisque cette fois il est utilisé massivement et délibérément dans le cadre d'une guerre de haute intensité.

Nous pouvons distinguer deux points majeurs : l'attaque sur les serveurs, visant à désorganiser l'adversaire, et la désinformation.

Une attaque de serveurs, qui peut sembler anodine dans un contexte de guerre ouverte, a en

réalité les implications très concrètes. L'attaque par les Ukrainiens de la plateforme comptable de distribution d'alcool russe Egais, début mai, pourrait avoir occasionné une perte de 28 millions de dollars de droits d'accises pour la Russie, soit l'équivalent de quatorze chars T-80. L'enjeu est donc très concret. Je ne parle même pas de l'attaque informatique du satellite européen KA-SAT, en mai dernier, dont les Russes sont accusés. L'attaque de serveurs constitue donc un risque majeur, et nous devons être à la pointe sur cet aspect de la cybersécurité.

Le second volet de la cyberguerre est celui du renseignement et de la désinformation, dans laquelle les Russes sont très avancés.

Cependant, force est de constater que, dans ce conflit, la dimension cyber n'a pas encore été déterminante au point de désorganiser massivement les opérations ennemies. Les Russes et les Ukrainiens résistent, malgré des attaques répétées et des campagnes massives de désinformation. Aussi, n'avons-nous pas surestimé la dimension cyber dans un contexte de guerre de haute intensité ?

**M. Christophe Blanchet (Dem).** Vous avez évoqué la réserve, un sujet sur lequel planche, au niveau du ministère des armées, un groupe de travail auquel je participe. Vous avez notamment souligné ses limites dans le domaine cyber. Avez-vous des propositions d'amélioration ?

On distingue la réserve opérationnelle de premier niveau (RO1), la réserve opérationnelle de deuxième niveau (RO2) et la réserve citoyenne. Auquel de ces niveaux envisageriez-vous l'opérabilité des réservistes dans le cyber ?

Lors d'une audition, nous avons évoqué le fonctionnement des communautés et le rôle des influenceurs. Ces derniers peuvent, en un clic, transmettre une information à 30 000 abonnés d'un coup. Ne pourrions-nous pas mobiliser ces personnes qui, pour servir leur pays, seraient prêtes à diffuser une information gratuitement, bénévolement ? Ce n'est sans doute pas du cyber, mais cela s'en rapproche. Réfléchissez-vous à une éventuelle collaboration avec des influenceurs ? Comment pourrions-nous la structurer ? Serait-il envisageable de confier la gestion d'une communauté de ce genre à un réserviste citoyen ?

**Mme Anne Le Hénanff (HOR).** Vous avez évoqué les différents types de couches informatiques et expliqué que les Américains aidaient activement l'Ukraine à s'équiper et à se protéger. L'Europe ouvre donc les vannes aux Américains pour ce qui est du matériel informatique, avec tout ce que cela induit. Dans le même temps, nous essayons de définir le cadre d'une politique de souveraineté numérique européenne et de contrer l'esprit de conquête des Américains, que nous observons notamment sur le territoire français, dans différentes organisations telles que les chambres consulaires. Comment appréhendez-vous cette double approche ? Certes, nous devons protéger un pays en guerre et avons donc besoin de matériel et de spécialistes compétents dans un domaine où les Américains sont indéniablement experts. Mais ce faisant, même si l'Ukraine n'est pas membre de l'Union européenne, nous facilitons l'accès des États-Unis au territoire européen.

**Général de division Aymeric Bonnemaison.** Nous le voyons nous-mêmes sur les réseaux

sociaux, Monsieur Jacques : chaque utilisateur développe autour de lui des sphères de proximité ou d'affinité, notamment idéologique, avec d'autres utilisateurs auxquels il envoie des messages et qui vont surenchérir. C'est d'ailleurs tout le problème de la radicalisation par le biais des médias. Dans le cadre d'un conflit, c'est un peu la même chose : chaque partie active les relais qui lui sont proches. Pensez-vous qu'un message russe parviendra à persuader un Ukrainien ou même un Occidental que cette guerre est une bonne chose ? Je ne suis pas sûr que les Russes s'investissent beaucoup dans ce genre de contestation, qui leur ferait perdre beaucoup trop d'énergie. Pour eux, l'enjeu est peut-être plutôt de convaincre les autres pays, ceux qui ne sont pas occidentalisés ou qui rejettent une forme de domination de l'Occident, qui pourraient leur servir de relais dans les enceintes internationales. Il y a une tendance naturelle à constituer des bulles, et notre étude a permis de constater que ces différentes bulles ne se parlent pas, ne se contestent pas. On observe malheureusement la même chose à l'échelle de notre pays : si le débat a lieu à l'Assemblée nationale, il est en réalité assez peu présent sur les réseaux sociaux.

Madame Martinez, je découvre ce chiffre de 65 % que vous avez cité, qui me surprend et m'inquiète un peu. Je ne pensais pas que nous en étions là. Dépendant du ministère des armées, je ne représente pas l'État dans son ensemble et ne peux donc répondre que partiellement à votre question mais, comme je le disais, nous devons mener un gros travail d'acculturation et d'éducation des différents acteurs concernés par ces problématiques. Nous nous heurtons toutefois au principe de réalité : certaines entreprises n'ignorent pas qu'elles peuvent être attaquées mais n'ont pas d'argent pour financer leur protection et ne savent pas comment s'organiser. C'est ici qu'intervient l'Anssi, qui a entrepris de labelliser des sociétés chargées d'apporter aux entreprises des conseils, voire de petites solutions. Il en émerge beaucoup en ce moment. Dans l'écosystème français du numérique qui est en train de se constituer, de nombreuses solutions pratiques sont ainsi développées pour donner aux entreprises, y compris petites – car les grands groupes ne sont pas les seuls à devoir se protéger – une première capacité de réponse. Par ce biais, nous améliorons notre résilience globale.

Madame Serre, j'ai l'impression que beaucoup de gens sont conscients du rôle des Gafam et de la nécessité d'exercer sur eux un contrôle politique. L'Union européenne s'est un peu réveillée à ce sujet. S'il est difficile de déstabiliser ce monopole, je vois aussi émerger, depuis cinq ou six ans, des capacités françaises dans ce domaine – j'ai encore pu le constater récemment à l'European Cyber Week ou aux Assises de la cybersécurité à Monaco. Des jeunes ayant la fibre nationale, dont certains ont d'ailleurs déjà servi dans notre ministère, montent des boîtes, des « jeunes pousses », sans chercher à se faire racheter tout de suite par un grand groupe américain, comme de nombreux entrepreneurs le souhaitaient auparavant. Ils sentent certes qu'il y a un marché à conquérir, mais ils sont aussi sensibles à la nécessité d'une souveraineté française, voire européenne dans ce domaine. Nous devons accompagner ces pépites, notamment dans le cadre des levées de fonds, et les protéger de la prédation.

Lors de la présidence française de l'Union européenne, mon prédécesseur a organisé la première rencontre de tous les cybercommandeurs européens. Nous nous réunissons désormais une à deux fois par an : vous voyez donc que nous sommes à la manœuvre pour faire émerger des solutions européennes. Nous aimerions aussi créer des capacités

d'intervention européennes : lorsqu'un pays rencontrerait une difficulté, l'un de ses partenaires pourrait mobiliser un groupe d'intervention cyber (GIC) pour lui venir en aide. Cela nous permettrait d'empêcher les Américains d'occuper l'espace vide. Les États-Unis sont en effet venus aider des pays ayant besoin d'une réassurance, notamment certains pays frontaliers de la Russie ; dès lors, il sera compliqué de les faire partir… Quoi qu'il en soit, il est important de développer une offre de services, une capacité à aider d'autres pays – c'est aussi une forme de diplomatie d'accompagnement et une contribution à la construction européenne –, ce qui nécessite évidemment des moyens. J'ai aujourd'hui une capacité comptée de GIC, qui doivent déjà traiter nos problèmes nationaux et pourraient être mobilisés pour renforcer l'Anssi en cas de crise majeure dans notre pays.

Monsieur Fiévet, il existe déjà une Agence européenne de cybersécurité, l'Enisa. Beaucoup d'initiatives et de travaux sont en cours. Je l'ai dit, le cyber avait autrefois un petit côté secret, régalien, mais les notions de partage et d'entraide dans la lutte informatique défensive sont aujourd'hui largement admises.

Vous vous demandez, Monsieur Berteloot, si nous n'avons pas surestimé le cyber. Personnellement, je ne le pense pas. Nous l'avions déjà écrit dans notre livre, qui n'est pourtant pas récent, et je crois vous l'avoir démontré tout à l'heure : le cyber ne fait pas tout, mais cela ne l'empêche pas d'être présent avant les conflits, pendant, même si c'est un peu moins, et enfin après, sous la forme de l'espionnage, voire du pillage. Même s'il ne permet pas de résoudre toutes les guerres, le cyber est un véritable outil de puissance : il faudra donc intégrer à la LPM tout ce dont nous aurons besoin pour devenir plus résilients dans ce domaine. Je me reconnais d'ailleurs dans presque tous les objectifs déclinés dans la revue nationale stratégique : au-delà de l'objectif stratégique n° 4, intitulé *« une résilience cyber de premier rang »*, je suis concerné par l'intégration du combat, les nouveaux champs, la liberté de manœuvre multimilieux. Le cyber intéresse l'ensemble de la société. Quand les armes parlent, il est un petit peu moins prépondérant, mais il reste un acteur.

S'agissant des réserves, Monsieur Blanchet, je ne peux pas vous apporter de réponse immédiate car nous sommes en train d'y travailler. Nous ne découvrons pas le sujet : nous avons déjà de belles expertises, notamment une réserve de compétences qui vient renforcer notre Cassi (centre d'audit de la sécurité des systèmes d'information) et notre Calid (centre d'analyse en lutte informatique défensive). Il est sans doute possible d'aller plus loin, d'agréger des compétences, mais je ne voudrais pas vous livrer des réflexions qui ne sont pas encore tout à fait consolidées en interne. La constitution de réserves permettra aussi de renforcer, dans les territoires, la nécessaire acculturation dont je parlais tout à l'heure. Nous commençons à tenir un tel discours aux entreprises, qui sont nombreuses à se sentir concernées par ce sujet.

S'agissant de la mobilisation de la réserve citoyenne et des influenceurs, je suis partagé. Cette démarche pourrait s'avérer tout à fait bénéfique mais, comme je l'ai déjà dit tout à l'heure, l'influence se manie avec prudence. En général, l'influenceur est un homme très libre ; mais s'il intervient en tant que réserviste, il porte la parole des armées, il me représente, et je devrais assumer tout ce qu'il dira en dehors du champ de la réserve. Nous avons pensé à solliciter des influenceurs pour le recrutement : la réserve citoyenne telle qu'elle avait été initialement

conçue par l'amiral Coustillière a engagé un travail à ce sujet, et je vous avoue que j'ai moi-même déjà commencé à étudier la question. Encore une fois cependant, la mobilisation d'influenceurs engagera notre parole.

**M. Christophe Blanchet (Dem).** Quel est l'état de vos réflexions s'agissant de la RO2 ?

**Général de division Aymeric Bonnemaison. E**lles sont moins avancées, et l'état-major des armées a entamé une étude d'ensemble pour mieux exploiter la réserve de 2e niveau (RO2), qui regroupe, sous un régime de disponibilité obligatoire, tous les anciens militaires, dans la limite des cinq années suivant la cessation de leur état militaire.

**Mme Josy Poueyto (Dem).** Vous disiez tout à l'heure que vous manquiez de femmes. On peut se demander pourquoi, et ce qu'il est possible de faire pour les inciter à vous rejoindre. Peut-être des influenceuses ?

**Général de division Aymeric Bonnemaison.** Il y a déjà beaucoup d'influenceuses. C'est dans la couche sémantique que la féminisation pose le moins de problèmes, car les profils sont moins techniques – nous recrutons des psychologues ou des gens qui ont fait du marketing, par exemple.

S'agissant plus généralement de la féminisation de nos effectifs, je vous ai déjà parlé du dispositif des cadettes. Avec le directeur général de l'enseignement scolaire, nous réfléchissons aussi à l'idée d'intégrer systématiquement une femme dans les équipes de Capture the flag : cela montrerait aux jeunes filles que ce domaine est abordable et pourrait faire naître la motivation. Mais ces réflexions ne sont pas encore abouties.

**M. Jean-Louis Thiériot (LR).** Bien que je comprenne la préoccupation de M. Blanchet, je souscris entièrement à vos remarques s'agissant de la nature des influenceurs. Ce sont parfois des électrons libres, et nous ne savons pas forcément ce qui pourrait en sortir. Je pense, mais cela reste un sentiment, que ce travail devrait plutôt être mené par les services spécialisés, de sorte que les agissements de ces influenceurs ne puissent être directement attribuables.

**M. Aurélien Saintoul (LFI-NUPES).** L'articulation entre le Comcyber et le renseignement est-elle optimale ?

**Général de division Aymeric Bonnemaison.** Je vais vous surprendre : dans le domaine technique, les échanges entre le Comcyber et les différents services de renseignement se passent bien, grâce notamment au C4, où nous nous voyons très régulièrement et où l'expertise des services de renseignement nous aide à la caractérisation et à l'imputation technique des attaques que nous avons repérées. Le fait que certaines personnes, dans le domaine cyber, passent facilement d'un monde à l'autre facilite également nos relations. C'est d'ailleurs quelque chose que nous essayons de mettre en avant afin d'attirer les profils que nous voulons recruter. Beaucoup se sentent vite enfermés et n'ont pas envie de s'engager pour vingt ans dans les armées : nous leur montrons que des parcours croisés sont possibles. Cela nous incite à être d'autant plus prudents en matière d'influence.

**M. le président Thomas Gassilloud.** Merci, mon général, pour ces échanges.