ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition du général de division aérienne Didier Tisseyre, général commandant la cyber défense sur le thème « le cyber, nouvel espace de conflictualité ».

Mercredi
4 mars 2020
Séance de 9 heures 30

Compte rendu n° 40

SESSION ORDINAIRE DE **2019-2020**

Présidence de Mme Françoise Dumas, *présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures trente-cinq.

Mme la présidente Françoise Dumas. Nous avons le plaisir de recevoir le général Didier Tisseyre, commandant de la cyberdéfense à l'État-major des armées, connu sous l'appellation de COMCYBER. Le sujet qui nous préoccupe aujourd'hui est appelé à prendre une place de plus en plus considérable et prééminente, et je me réjouis que nous puissions consacrer cette dernière séance de notre cycle géostratégique à l'émergence de l'espace cyber comme nouveau champ de conflictualité. Les chiffres de l'actuelle loi de programmation militaire (LPM) sont éloquents : est prévue la création de 1 500 postes dans le domaine de la cyberdéfense et du numérique dont 1 000 cyber combattants supplémentaires afin de porter leur nombre total à 4 000 personnels vers 2025. Parmi ces effectifs, 500 sont appelés à être placés sous l'autorité organique du COMCYBER, le reste étant sous son contrôle opérationnel.

Vous nous expliquerez, général, quelle est votre feuille de route pour la mise en œuvre des ambitions de la LPM, et quel premier retour d'expérience vous en tirez afin que nous puissions en tenir compte dans l'optique de l'actualisation de la LPM prévue en 2021. Nous attendons également de vous un tableau des rapports des forces en présence et que vous nous expliquiez leurs évolutions récentes ainsi que les menaces dont elles sont porteuses. Dans ce domaine technique et par nature moins visible que les formes traditionnelles de la guerre, vous pourrez illustrer vos explications par quelques exemples récents qui nous permettront de mieux saisir ce que sont les opérations cyber autant défensives qu'offensives. Notre commission a d'ores et déjà commencé à travailler sur ces thématiques puisqu'en juillet 2018, un peu avant la promulgation de la LPM, nos collègues Alexandra Valetta Ardisson et Bastien Lachaud nous avaient présenté un excellent rapport d'information sur la cyberdéfense. Nos commissaires s'attachent en effet à suivre de près toutes ces évolutions technologiques – et elles sont particulièrement rapides avec le numérique – afin de préparer nos travaux sur la programmation et d'attirer constamment l'attention de la ministre sur les enjeux à l'œuvre. C'est le sens des travaux d'Olivier Becht avec Thomas Gassilloud sur la numérisation des armées, et avec Stéphane Trompille sur l'espace. C'est aussi celui de la mission que nous avons confiée à Claude de Ganay et Fabien Gouttefarde sur les systèmes d'armes létaux autonomes (SALA). Nous serons donc très attentifs aux points de vigilance que vous voudrez bien nous souligner pour la prise en compte de ces évolutions technologiques dans le champ de la cyberdéfense.

Général de division aérienne Didier Tisseyre, général commandant la cyberdéfense. Je vous remercie vivement de votre invitation à m'exprimer au sujet du cyberespace, cet espace de conflictualité, et pour évoquer avec vous ses enjeux, en particulier pour la défense de notre pays. Je vous propose trois temps dans mon propos liminaire, que j'émaillerai d'un certain nombre d'exemples. Le premier temps m'amènera précisément à parler de cette conflictualité associée au cyberespace et de ce qui la caractérise. J'expliquerai ensuite comment cette conflictualité touche les questions de sécurité et de défense. Je traiterai enfin, plus spécifiquement, du commandement de la cyberdéfense : sa dynamique, son action, ses responsabilités.

La conflictualité dans le cyberespace est liée au numérique, qui est partout, dans toutes les activités humaines, et qui soutient l'ensemble des métiers – qu'ils soient privés ou publics –, et des individus. À la base, évidemment, le but est de créer du progrès, relier les uns et les autres, faciliter ces activités. Ces mécanismes techniques qui permettent de relier les uns et les autres – et en quantité : une personne vers une multitude – de contracter l'espace et le temps dans la transmission de l'information et de partager énormément d'éléments sont une

chance mais aussi un risque. Certains ont clairement identifié ce risque et la valeur des données personnelles, par exemple, que d'aucuns mettent peut-être trop imprudemment sur internet. Ils ont vu qu'ils pouvaient tirer profit de ces liens entre les individus, de tout ce qui peut transiter par le cyberespace. Celui-ci attire tout type de convoitise, tout type de cybercriminalité. Cela facilite bien sûr l'espionnage, puis en élargissant, l'influence, le sabotage et la déstabilisation… Ces mots existaient déjà depuis très longtemps, mais ils prennent une dimension tout autre en raison des caractéristiques même du cyberespace.

Il est important de comprendre que le cyberespace est totalement façonné par l'homme. Par rapport aux espaces aériens, terrestre, maritime et même spatial, il est le seul à avoir été construit par l'homme, et il ne cesse d'évoluer. Cette évolution rend difficile l'identification de ses contours, actuels et futurs. Au départ, il est plutôt basé sur une gouvernance technique, dans laquelle les États ne sont pas forcément présents. Mais aujourd'hui se pose la question de la présence des États et de l'ensemble des opérateurs que l'on peut y retrouver. Le cyberespace est ainsi comme d'autres espaces, d'autres médias : un champ d'expression des rivalités entre États, entre groupes, entre entreprises, et un champ d'action pour un certain nombre de criminels. Tous ceux qui souhaitent l'utiliser à leur profit pour imposer leur volonté se servent des difficultés et des fragilités en matière d'organisation et de technologie, mais aussi parfois du manque de connaissance de la part de ses utilisateurs. Vous le voyez, de telles conflictualités présentent des enjeux de sécurité et de défense.

Je prends deux exemples. À l'été 2019, dans un cadre structuré, le Pentagone aux États-Unis a demandé à un certain nombre de hackers – hackers au sens plutôt sympathique de *« bidouilleur »* – de tester des systèmes et leur sécurité. En 48 heures, ces hackers ont réussi à prendre la main sur les systèmes numériques déployés au sein d'un avion F-15. On voit tout ce que cela peut avoir comme effet dans le cadre d'opérations utilisant ces moyens très modernes équipés d'armements mortels… Même sur des matériels très pointus, très évolués – même si le F-15 n'appartient pas à la toute dernière génération des avions de combat –, il existe des vulnérabilités. Ces systèmes d'armement ont été conçus il y a dix ou même vingt ans, à une époque où la cyberdéfense n'avait pas la même portée qu'aujourd'hui et où l'on n'avait pas encore la connaissance des vulnérabilités associées au cyberespace. Il y a un rattrapage à faire, et il est parfois compliqué.

Autre exemple assez emblématique de ce que l'on peut faire en matière d'actions offensives dans le cyberespace : le fameux virus Stuxnet, utilisé il y a un certain nombre d'années pour freiner le déploiement et le fonctionnement de centrifugeuses en Iran. On imagine que pour atteindre ces centrifugeuses – en fait les systèmes informatiques qui permettent de les contrôler –, il a fallu tout un travail de renseignement, de connaissance, d'ingénérie, afin que ce logiciel agisse à longue distance. Une coordination et une planification extrêmement pointues de l'opération ont permis qu'elle ait un réel effet pour ralentir les capacités d'un pays.

On voit que tout rapport de force doit intégrer cette notion de cybersécurité, de cyberaction : celui qui ne le fait pas part avec un désavantage par rapport à ceux qui le font et qui n'appliquent pas les mêmes règles éthiques que nous. Il faut donc anticiper ces risques, se montrer résilients afin de protéger tout ce qui est essentiel dans le territoire national. C'est la volonté du ministère des armées.

Je pourrais prendre d'autres exemples dans l'armée de Terre ou la Marine mais, en tant qu'aviateur, je suis évidemment très sensible au déploiement de la puissance aérienne et du feu aérien. L'apparition de l'aviation a été, en bon français, un *game changer*, qui nous a apporté une capacité d'action au-delà des lignes ennemies, une capacité de frapper la logistique, d'acquérir des informations, d'obtenir du renseignement, de mieux calibrer les tirs d'artillerie. Oui, celui qui disposait de ces capacités avait un avantage sur les autres. Dans

toutes les opérations interarmées, l'acquisition de la supériorité aérienne, de manière continue ou ponctuelle, est un prérequis indispensable. Celui qui n'a pas cette supériorité aérienne se trouvera dans une situation beaucoup plus difficile et devra faire face à la capacité de l'adversaire en matière de renseignement, en matière de frappe dans la profondeur ou sur la ligne de front.

Le lien est évident avec cette nouvelle capacité liée au numérique et à la cyberdéfense : celui qui maîtrisera le cyberespace aura un avantage, non seulement pour se protéger, mais aussi pour assurer sa supériorité opérationnelle. C'est ce qui est fait par le ministère des armées sur nos théâtres d'opérations, au Levant, au Sahel. Les capacités dont nous disposons en matière de cyberdéfense sont le fruit d'un travail de plusieurs années et sont utilisées pour préserver nos capacités et nos systèmes d'armes très numérisés. Elles permettent un combat collaboratif, l'échange des informations en temps réel, donc des opérations combinées, imbriquées, intégrées, mais également un blocage de l'adversaire, notamment - c'est ce qui a été fait contre Daech - de sa propagande et de la préparation de ses opérations contre nos forces déployées en opérations.

Dans l'histoire, on retrouve ces mécanismes de stratégie militaire et de leur application. Selon le stratège chinois Sun Tzu « le meilleur savoir-faire n'est pas de gagner cent victoires dans cent batailles, mais plutôt de vaincre l'ennemi sans combattre ». Avec le cyber et les attaques systémiques, certains imaginent faire tomber un système complet. Reprenons l'exemple des F-15 américains, potentiellement vulnérables à des attaques : si vous les empêchez de décoller, vous avez forcément un avantage important et, à la limite, avant même de les avoir déclenchées, vous avez gagné les batailles, vous avez gagné la guerre.

Aujourd'hui, un autre stratège, américain cette fois et du XX^{e} siècle, John A. Warden III, voit les institutions, les structures et l'ennemi comme un système de plusieurs cercles. Il a décrit ces cercles. Vous avez évidemment les forces militaires déployées pour assurer la protection et les actions ; les populations aussi ; les infrastructures qui sont aujourd'hui des éléments importants – comme le médical, l'énergie, en plus des routes, ports, aéroports – et qui sont ciblées par certains ; dans le quatrième cercle, on trouve des fonctions organiques essentielles – production d'énergie, fourniture de carburant, approvisionnement en nourriture ; et dans le dernier, les fonctions de commandement, étatiques, régaliennes, de gouvernance et de très haute direction. Dans la conflictualité entre les armées et entre les États, on trouve toujours l'application de ces principes pour savoir si l'on va cibler des forces militaires déployées ou directement l'endroit où l'on prend les décisions, pour paralyser ou empêcher ces décisions. Au XX^{e} siècle, on ciblait l'un ou l'autre de ces cercles. Avec le cyber, on peut cibler la totalité et mener une action combinée contre les forces armées, les populations, les infrastructures essentielles du pays, mais aussi contre des systèmes de décision. Cette double action s'exerce aussi sur les populations : sur leur quotidien, sur l'ensemble de leurs systèmes d'information, mais aussi sur leur positionnement, au travers des réseaux sociaux. C'est donc un véritable risque existentiel qui pèse sur nos sociétés, confrontées à ceux qui savent utiliser le cyberespace pour bloquer nos systèmes et imposer leur volonté.

Les impacts peuvent être très forts. Aujourd'hui on découpe les actions dans le cyberespace entre plusieurs problématiques. D'abord, qui peut nous attaquer ? Un État ? Un groupe potentiellement rattaché à un État, mais pas forcément officiellement ou en uniforme ? Ses individus ? Ensuite, quelles sont les techniques, les tactiques, les procédures utilisées ? Faisons une comparaison avec des cambrioleurs : ils ont leurs astuces, leur stratégie. Certains vont passer par les toits, certains par la fenêtre, d'autres par la porte. Les cyberattaquants appliquent aussi leurs propres stratégies. Ces stratégies sont caractéristiques d'un certain nombre de groupes, et il est important de bien les connaître pour savoir comment réagir, s'il

faut protéger les toits, les sous-sols ou les fenêtres. Dans le cyberespace, on doit tout protéger, être capable de tout défendre, parce qu'il suffit que l'attaquant trouve une entrée pour pénétrer dans votre système. Fort des réponses à « qui nous attaque ? » et « comment ? », se pose ensuite la question de l'impact et des effets. Ces effets sont de trois types. Cela peut être un effet d'entrave, de perturbation du fonctionnement d'un système : j'évoquais un avion qu'on empêcherait de décoller. Mais on peut aussi bloquer une centrale d'énergie pour déstabiliser et entraver la manœuvre de l'ennemi. La deuxième action possible, c'est de capter des données ; parce qu'on fait de l'espionnage économique, on récupère l'ordre de bataille de l'autre pour pouvoir se prépositionner. La troisième finalité est de modifier la perception de l'autre, de le leurrer et d'influencer sa vision. Tels sont les trois objectifs visés par les attaques cyber.

Dans le cadre de nos opérations, nous intégrons ces trois dimensions. Nous faisons particulièrement attention aussi à nos informations et à nos systèmes. Nous essayons – et pour l'instant, nous y réussissons – d'assurer la confidentialité de ces données qui sont essentielles à notre manœuvre et à notre métier, mais aussi leur intégrité. J'ai parlé du risque de modification : leur intégrité est essentielle. Et, on a tendance parfois à l'oublier, nous veillons à la disponibilité des données. Celle des traitements est également essentielle. Pour le cyberdéfenseur, ce sont des éléments à intégrer et pour lesquels il faut déployer des mécanismes de sécurité.

On peut avoir l'impression que l'attaquant fait tout ce qu'il veut, qu'on est démuni face à lui. Il existe tout de même un cadre, de plus en plus précis. Le droit international s'applique au cyberespace. Il est toutefois difficile de savoir quelles sont les modalités précises de son application. Les États ou les groupes reconnaissent-ils ces principes ? De quelle manière les appliquent-ils ? Se sentent-ils concernés et engagés par ces principes ? À une époque, un manuel de référence – le manuel de Tallinn – expliquait, à la suite d'un groupe de travail multinational, comment appréhender ces notions de cyberespace. Désormais, deux groupes de travail y réfléchissent dans le cadre de l'ONU, l'un présidé plutôt par les Américains, le second plutôt par les Russes. Au plan national, à l'initiative du ministère des armées, un rapport sur l'application du droit international aux opérations cyber, décrit les mécanismes de perception par la France des attaques cyber sur son territoire contre ses systèmes. Qui nous attaque ? Comment peut-on réagir ? Quels sont les principes de légitime défense, les principes de souveraineté numérique – c'est très détaillé – mais aussi les principes applicables aux opérations cyber sur les théâtres d'opérations : quel est leur cadre ? Comment sont-elles réglementées ? Quels sont les principes de proportionnalité, de disponibilité et de discrimination ?

Quand on parle d'opération cyber, on imagine Tom Cruise sautant en parachute avec un ordinateur portable qui lui permet de communiquer directement et de déclencher énormément de choses pour qu'il remplisse sa « mission impossible ». Dans la réalité, au risque de vous décevoir, une opération cyber se prépare très longtemps à l'avance. Ses effets peuvent être immédiats : il suffit qu'on déclenche ce qui a été prépositionné pour avoir un effet immédiat et très large. Mais pour obtenir cet effet, il faut l'avoir préparé très longtemps à l'avance. Il faut avoir une connaissance très précise des infrastructures informatiques de la cible pour identifier de quelle manière l'atteindre. Il faut prépositionner ses équipements pour réaliser l'action que l'on souhaite mener : les phases de planification et de renseignement sont donc très importantes.

On distingue parfois les temps de paix, de crise et de guerre. Je vous assure que, dans le cyberespace – je pense que vous le savez –, nous ne sommes pas dans un temps de paix : il y a de nombreuses crises, et, d'une certaine manière, la guerre cyber a déjà commencé. Certains déploient leurs outils et se prépositionnent pour pouvoir le jour J, au moment où ils

appuieront sur la touche « *Enter* », déclencher immédiatement les éléments. Or une fois qu'on est paralysé, il est trop tard pour réagir.

Au sein du ministère des armées, comment se positionne le commandement de la cyberdéfense que j'ai l'honneur de commander depuis septembre dernier et dont j'avais auparavant été numéro deux pendant deux ans ? Créée en 2017, cette entité est en fait le fruit de dix ans de montée en puissance, ce qui nous renvoie à 2007 et à la cyberattaque de l'Estonie par un voisin qui a voulu réagir au déplacement d'une statue. Cet événement a marqué une prise de conscience internationale : si quelqu'un a des cyber capacités et souhaite les utiliser, il peut provoquer un impact très fort sur un État. De nombreux pays se sont alors préoccupés de ces menaces cyber et ont développé des éléments de défense.

Atteindre et développer cette capacité que nous possédons aujourd'hui au sein du ministère et dont dispose le commandant de la cyberdéfense relève d'une volonté politique. Les moyens alloués par la loi de programmation militaire ont permis d'engager les budgets et les ressources humaines nécessaires pour développer ces capacités.

Des documents précis de doctrine – notamment des éléments qui ont été rendus publics sur la doctrine, sur les opérations de lutte informatique offensive à des fins militaires – ont également fixé le cadre et les objectifs de notre action. Les missions du commandement de la cyberdéfense sont donc la protection et la défense des capacités du ministère des armées, et comprennent également des possibilités d'action dans le cyberespace sur les théâtres d'opérations. Je suis le contrôleur opérationnel de l'ensemble des opérations dans le cyberespace : opérations défensives au profit du ministère des armées et opérations offensives au profit de la nation, en fonction des choix politiques qui sont faits. Dans la chaîne de responsabilité, le Président de la République, chef des armées, décide d'une action cyber au même titre que d'une action militaire.

On est dans la continuité du domaine. Par exemple, nous avons mené des actions offensives en coalition contre Daech sur les théâtres d'opérations, au même titre que des actions ont été menées de manière plus traditionnelle avec ces mêmes coalitions, pour réduire la taille et la portée des actions de Daech. Dans le cyberespace, nous avons notamment ciblé tout leur appareil de propagande, identifié où étaient localisés les serveurs, pénétré ces serveurs, effacé les données, et bloqué ces serveurs pour que la propagande ne puisse plus être diffusée. Tout cela a été réalisé dans une approche plus globale d'identification des contenus terroristes avec le relais de la plateforme Pharos (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) du ministère de l'Intérieur – autorité administrative des opérateurs de l'internet – pour déréférencer un certain nombre de contenus de propagande terroriste.

Nous sommes confrontés à des défis technologiques, vous l'imaginez, mais aussi à des défis de captation de l'innovation. Dans un espace cyber qui évolue très vite, nous avons besoin de pouvoir capter cette innovation avec des procédures et des processus rapides. Nous le faisons notamment au travers d'une Cyberdéfense *Factory* installée à Rennes. Surtout, nous devons relever le défi des ressources humaines. Les cyber combattants ne sont pas uniquement des Bac + 5 en informatique – il en faut, bien évidemment –, mais aussi des techniciens, des personnes ayant un esprit très analytique, géopolitique, pour comprendre ce cyberespace. Ce sont également des psychologues, des sociologues pour comprendre cette couche cognitive : j'évoquais précédemment les réseaux sociaux, c'est évidemment essentiel. En fait, la meilleure équipe de cyber combattants est une équipe mixte, polyvalente, bien évidemment féminisée. Cela aussi est essentiel : nous avons 15 % de taux de féminisation dans le COMCYBER, ce qui est à noter dans un domaine très technique. Nous nous appuyons aussi beaucoup sur des réservistes opérationnels.

Je conclurai en disant que l'humain est fondamental. On a l'impression que le cyberespace n'est que de la technologie, mais, en fait, c'est l'humain, par son implication, par des formations régulières tout au long de son contrat et de sa carrière, qui permet de répondre dans ce domaine très évolutif.

Mme Jacqueline Dubois. Aucun traité international ne régit à ce jour le cyberespace. Quelle est la position du Commandement sur la pertinence de légiférer dans ce domaine ? Quels sont les États réticents à l'établissement d'un document universel ? Et quelle pourrait être l'autorité ou l'organisation internationale en charge de son application ? J'ai bien conscience que cela doit être extrêmement complexe.

M. Charles de la Verpillière. S'agissant de la robustesse ou de la vulnérabilité des systèmes qui peuvent faire l'objet d'attaques cyber, on voit bien qu'il faut que nous protégions non seulement nos systèmes militaires – par exemple le programme SCORPION, très important à l'échelon tactique –, mais également des systèmes civils. Parmi les systèmes civils, il y a ceux des services publics. Je pense à tout ce qui concerne l'électricité – RTE, Enedis… – mais également aux hôpitaux. Là, l'État peut encore avoir la main. En revanche, cela se complique avec les grands systèmes privés, notamment les banques. On peut créer le désordre en sabotant leur système, mais on peut aussi procéder à du *phishing* – de l'hameçonnage – trouver des données gênantes pour certains particuliers, etc. Pouvez-vous nous en dire plus sur la protection de ces systèmes privés en prenant l'exemple des banques ? Travaillez-vous avec les grands groupes bancaires français et étrangers ?

M. Jean-Pierre Cubertafon. L'un des enjeux majeurs en matière de cyberdéfense est le maintien au plus haut niveau de notre capacité opérationnelle dans le cyberespace. Cela nécessite notamment une attention particulière portée au recrutement, à la formation et à la fidélisation des cybercombattants. Sur ces trois aspects – recrutement, formation et fidélisation – je souhaiterais savoir s'il existe une spécificité du cybercombattant. Si tel est le cas, les outils dont disposent nos armées pour recruter, former et fidéliser nos soldats sont-ils adaptés ?

M. Olivier Becht. Vous nous avez clairement indiqué que les États procèdent au prépositionnement des armes sur les réseaux à travers des bombes logiques, que nous avions déjà analysées dans le rapport sur la numérisation des armées que j'ai rédigé avec mon collègue Thomas Gassilloud. Je souhaite vous poser une question relative à l'intelligence artificielle (IA). On sait qu'on essaye de greffer sur ces bombes logiques des programmes d'IA, de sorte que demain, dans le cyberespace, se déroulera une bataille entre les IA intelligentes et positives alliées qui tenteront de détecter les bombes logiques ennemies, qui seront elles-mêmes équipées d'IA qui leur permettra de se dissimuler des IA qui chercheront à les débusquer… Où en est la France dans le développement de ces bombes logiques munies d'intelligence artificielle ? Pensez-vous que nous sommes à un stade qui nous permettra, demain, d'être meilleurs que ceux qui voudront nous frapper les premiers ?

M. Yannick Favennec Becot. Trois questions. Quelle est la nature des incidents cyber auxquels le COMCYBER a dû faire face en 2019 ? En France, les groupes États qui lancent des attaques cyber ne sont pas désignés : selon vous, l'attribution publique de ces attaques serait-elle nécessaire ? Enfin, en ce qui concerne les recrutements, mais également la fidélisation, quelles sont les difficultés que vous rencontrez compte tenu de la forte concurrence des entreprises privées pour recruter des experts en cyberdéfense ? De quels moyens disposez-vous pour faire face à cet enjeu ?

Mme Séverine Gipson. Cyberattaques contre TV5 Monde en 2015 ; *Macron leaks* ; ministère des armées piraté en 2017 : toutes ces attaques, pour ne citer qu'elles, proviennent de groupes de hackers russes sans qu'un lien hiérarchique avec l'État russe puisse clairement être établi. Le président Poutine a lui-même déclaré dans un sourire que les hackers sont

comme les artistes : incontrôlables. À l'heure où l'entente avec la Russie est indispensable, notamment sur le dossier syrien, comment avoir une relation diplomatique apaisée quand cet État laisse faire, voire encourage, ses propres citoyens à lancer des attaques hostiles contre nos démocraties ?

Général Didier Tisseyre. Tout d'abord, une réponse par rapport au droit et aux structures juridiques. Je vois deux aspects : le premier, c'est que la France puisse réagir comme elle le souhaite dans le respect du droit international et de ses principes – maîtrise de l'escalade, paix, stabilité internationale – jouer pleinement son rôle et assumer sa place dans le monde par rapport à ses engagements. Il faut donc dans un premier temps que le droit international, ou la manière dont il est compris par les uns et les autres, nous permette d'agir, notamment sur les théâtres d'opérations. Grâce aux lois de programmation militaire, un certain nombre d'éléments, gérés plutôt par l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, à laquelle nous sommes partie prenante, permettent de réagir légalement à une attaque. Je m'explique : on se fait attaquer, on identifie qui est l'attaquant – ce peut être un État – la possibilité nous est offerte de riposter et de faire stopper l'attaque. La loi nous le permet et les choses sont dites sur la scène internationale.

Alors que le manuel de Tallinn ne donne que des indications et n'est pas prescriptif, le rapport français dit clairement que l'attaque d'un État contre nos systèmes d'information est une atteinte à la souveraineté numérique de ces systèmes. Et en fonction du type d'attaquant, de la manière dont il est entré dans nos systèmes, de l'impact sur ces systèmes, le rapport décrit la palette des réponses – cyber, mais aussi économiques, politiques – dont nous disposons.

Il faut que cette compréhension de l'application du droit international au cyberespace, de ces principes et de leurs modalités d'application, soit partagée le plus possible. Je l'ai dit, il existe deux groupes au niveau de l'ONU : l'un, d'experts gouvernementaux, le GGE (*Group of Governmental Experts*), plutôt dirigé par les Américains. Même s'il n'a que 25 membres, il travaille beaucoup sur ces aspects de droit, car les Américains et d'autres y sont très attentifs et souhaitent que l'on cadre mieux ce que les uns ou les autres peuvent faire, de manière à ce qu'ils puissent réagir. Les États-Unis sont très présents dans le cyberespace : pour eux, c'est un moyen fort, à la fois de se protéger des attaques qu'ils peuvent subir et d'asseoir leur supériorité opérationnelle et leur influence dans le monde…

L'autre, l'*Open Working Group*, qui vient d'être créé, plutôt à l'initiative des Russes, compte une cinquantaine de membres qui réfléchissent aux mêmes problématiques, mais de manière un peu différente. Nous verrons sur quoi cela va déboucher et ce que l'ONU tirera de ces réflexions pour mieux cadrer le cyberespace, avec comme toile de fond un certain nombre d'articles de la Charte des Nations Unies, comme l'article 51, la légitime défense, etc. Ce qu'il faut, c'est que chaque État puisse mieux comprendre ce qu'il peut faire et ne pas faire s'il subit une cyberattaque.

Prenons le *hack back*, la riposte. En France, seul l'État peut mener une riposte, attaquer l'attaquant ; on ne donne pas aux entreprises la possibilité de le faire. Aux États-Unis, certains pensent que des entreprises pourraient le faire au nom du pays. C'est parce que les positionnements sont très différents qu'il importe de faire reconnaître un cadre juridique au niveau le plus élevé possible, notamment par l'ONU.

Le commandement de la cyberdéfense intervient dans son périmètre propre, par délégation de l'ANSSI, compétente pour le périmètre national. Donc pour toutes les infrastructures civiles, même si elles sont d'importance vitale, c'est l'ANSSI qui est à la manœuvre. Il n'en demeure pas moins que l'ANSII et le COMCYBER échangent énormément d'informations sur la connaissance de la nature de la menace. La ministre des armées a signé récemment une convention avec les huit principaux grands maîtres d'œuvre de la défense pour

faire en sorte d'élever collectivement le niveau de sécurité. Le ministère est bien sécurisé, et ceux qui veulent nous attaquer le feront de manière indirecte, en attaquant notre chaîne d'approvisionnement ou même les sous-traitants des grands industriels de la défense. Il faut donc que nous les protégions, et ces conventions définissent un cercle de confiance des échanges d'informations sur la nature de la menace. D'une certaine manière, même si le ministère des armées est dans son périmètre propre, on est de plus en plus dans une défense globale, d'autant que, tout le monde étant plus ou moins interconnecté, si quelqu'un est attaqué, l'autre peut l'être aussi. En résumé, si l'ANSSI est aujourd'hui à la manœuvre pour défendre le secteur et les services publics, il n'empêche que le commandement de la cyberdéfense peut y contribuer en cas de besoin, ne serait-ce qu'en matière d'assistance.

En effet, le combat entre les intelligences artificielles est essentiel. On peut les utiliser à la fois pour attaquer et pour défendre. Nous nous sommes mis en posture de le faire, avec le soutien de la DGA (Direction générale de l'armement), qui bénéficie pleinement de cet effort en ressources humaines que vous évoquiez, Madame la présidente, et travaille sur les algorithmes d'IA afin qu'ils puissent être utilisés au mieux à la fois pour l'offensif et le défensif. On a des laboratoires où on teste un certain nombre de choses… Je parlais tout à l'heure de capter l'innovation et cette innovation est souvent dans les start-up. Aussi brillants soient-ils, les ingénieurs de la DGA n'ont pas forcément toute l'information, toute la connaissance. Ainsi, la Cyberdéfense *Factory* est un lieu qui est ouvert, sous certaines conditions, à des start-up et des PME pour qu'elles viennent développer, tester leurs algorithmes notamment des algorithmes d'IA, avec des données représentatives de réseaux que nous avons en propre et que nous mettons à leur disposition. Cela leur permet d'y travailler et de développer, dans un cadre régalien, des logiciels et des mécanismes d'IA.

Nous avons bien conscience des enjeux et travaillons énormément dans le domaine des IA. Un comité d'éthique a été lancé au sein du ministère afin d'appréhender un certain nombre de sujets, notamment par rapport aux IA : jusqu'où peuvent-elles aller ? Jusqu'où peuvent-elles être automatisées ? Un des principes du ministère est qu'une IA doit toujours pouvoir être débranchée et ne doit pas conduire à des actions automatiques qui pourraient porter atteinte aux uns ou aux autres de manière indiscriminée. C'est le respect d'un des principes de droit international que j'évoquais, celui de discrimination entre une cible militaire et le monde civil. On ne souhaite pas, notamment au regard de l'impact que peut avoir une attaque cyber, qu'elle puisse se propager et attaquer ceux qui ne sont pas ciblés. On ne veut pas non plus que ces outils puissent être récupérés par certains, réutilisés contre nous. Nous portons une attention particulière à la non-prolifération de ce type d'outils. C'est un cadre très strict, mais il n'empêche pas que l'on travaille beaucoup et que nous soyons dans le peloton de tête.

Aujourd'hui, parmi les grands acteurs en matière de cyber, notamment ceux qui ont prouvé qu'ils pouvaient faire beaucoup de choses – directement parce que leur État l'a commandité ou indirectement par des groupes plus ou moins rattachés – il y a évidemment les Russes. Ils sont présents dans toute la palette de ce que l'on peut faire dans le cyber, des cyberattaques très ciblées jusqu'à l'influence au travers des réseaux sociaux : ils sont très forts. Les Chinois aussi et, selon les éléments que diffuse l'ANSSI, ils sont plutôt actifs dans l'espionnage économique. Mais dès lors qu'on entre dans un système pour voler de l'information économique ou industrielle, on peut faire autre chose, en entrant dans d'autres systèmes plus essentiels et mener d'autres actions. Nous y sommes très attentifs, comme nous sommes très attentifs à l'égard de pays comme l'Iran. Enfin, nous nous intéressons aux capacités américaines qui sont vraiment très développées, dans tous les domaines. Le Royaume-Uni et Israël sont aussi très pointus. En ce qui nous concerne, j'aurais tendance à dire, en particulier depuis le *Brexit*, que la France est la nation la plus forte dans l'Union Européenne en matière de cyberdéfense.

Pour les ressources humaines – le recrutement, la fidélisation et les spécificités de la formation des cybercombattants – évidemment sur le plan purement financier nous ne pouvons pas nous aligner sur les salaires que proposent des entreprises privées. En revanche, nous donnons du sens à l'action de ces spécialistes de la cyberdéfense : tout d'abord par la protection du ministère, de la nation, mais aussi par la possibilité de mener des actions fortes sur les théâtres d'opérations pour aller au cœur de la menace terroriste. Les sociétés privées ne mènent pas ces opérations offensives. Dans un cadre légal strict, nous offrons la possibilité de faire des choses qui ne sont possibles nulle part ailleurs, sauf de manière illégale et répréhensible.

Nous offrons aussi des formations spécifiques à la gestion de crise. Nous faisons évoluer notre système de formation pour l'adapter et mieux accompagner nos personnels. Aujourd'hui, il n'y a pas suffisamment de bac +5 spécialistes de cyberdéfense et nous allons donc prendre des BTS, que nous allons amener en quelques années au niveau souhaité, par des formations – internes ou en sous-traitance – et par la reconnaissance des acquis de l'expérience, en permettant ainsi l'obtention d'équivalences ou de diplômes. C'est attractif, motivant, et cela permet de fidéliser les personnels. Même s'ils optent ensuite pour l'industrie ou d'autres administrations, ils seront porteurs d'un niveau de cybersécurité et cela profitera à la collectivité.

L'attribution publique de l'origine de l'attaque relève de la décision politique, tandis que le commandement de la cyberdéfense et les services de renseignement travaillent à la caractérisation technique. À partir de la connaissance des modes d'action, des signatures des *malwares*, nous identifions le groupe spécialisé, le groupe APT – *Advanced Persistent Threat*, menace persistante avancée – à l'origine de l'attaque. Les programmeurs ont des habitudes, certains passent par la fenêtre, d'autres par la porte, et cela oriente leur identification. Des adresses IP spécifiques à certains modes d'action, avec leurs rebonds au plan international, nous permettent de caractériser l'attaquant et, forts de ces éléments et avec l'action complémentaire des services de renseignement, de proposer une attribution. Nous prévenons que c'est tel pays ou tel groupe qui nous attaque, avec un certain degré de certitude ; ensuite, le politique décide ou non de le révéler publiquement. En outre, cette attribution publique n'est pas une fin en soi. Une fois qu'on a dit « c'est lui qui nous a attaqués », que fait-on ? Riposte-t-on ? De quelle manière ? Il faut définir ce que l'on veut faire après et il y a des mécanismes pour cela. La France n'est évidemment pas opposée à une attribution publique : dernièrement, la ministre des armées a évoqué une attaque du groupe Turla contre les services du ministère.

Il existe aussi un mécanisme d'attribution publique, que la France a validé, dans le cadre de l'OTAN. Encore faut-il que tout le monde soit d'accord et que l'on sache à quoi cela va servir. Certains pensent qu'il est important de pointer du doigt et que désigner le responsable par le *name and shame* ou le *name and blame* – va le faire arrêter ses attaques. Mais un certain nombre d'attaquants vont nier et demander des preuves. Or les apporter contraindrait à dévoiler nos propres capacités de caractérisation et nos partenariats qui nous ont permis de mener à l'identification, donc à se fragiliser. Cela relève donc bien d'une décision politique.

S'agissant des Russes, en tant que commandant de la cyberdéfense, je travaille à la protection de nos infrastructures du ministère des armées et, bien évidemment, je me tiens au courant. Je le dis souvent, dans mes fonctions, je dois être paranoïaque, voir le pire dans toutes les situations et préparer notre défense. Mais en tant que citoyen, je suis pleinement attaché à la paix et la stabilité. On peut ne pas être naïf et chercher néanmoins comment dialoguer. Des canaux de dialogue et de désescalade potentielle ont été établis avec les Russes et sont testés. Il faut créer ce dialogue mais aussi aborder ensemble les volets de la

cybercriminalité. Il est ainsi possible d'échanger nos expériences dans l'organisation de grands événements comme les Jeux olympiques, En l'occurrence, cela se ferait plutôt sous l'égide de l'ANSSI, mais l'essentiel, ce sont ces occasions de dialoguer, de comprendre, d'expliquer, de mieux se connaître, tout en restant vigilant. On le voit, tout n'est pas binaire dans le cyberespace.

Mme Marianne Dubois. Mille cybercombattants doivent être recrutés d'ici 2025. Vous avez évoqué les compétences et la fidélisation, mais comment vous assurez-vous de l'état d'esprit des candidats ? Comment savoir s'il est compatible avec leur mission, s'ils sont dignes de confiance ?

M. Didier Le Gac. Le COMCYBER est-il organisé de manière très transversale, ou au contraire vos équipes sont-elles spécialisées selon les trois armées ? Pensez-vous par ailleurs que les moyens et les missions de la Marine présentent une vulnérabilité particulière ? Je pense notamment aux forces sous-marines, mais également à des bâtiments comme les FREMM (Frégates multimissions), qui sont des concentrés de technologie. Êtes-vous associé d'une manière ou d'une autre à la création prochaine du centre de cybersécurité maritime ? Ses missions iront au-delà de la défense, mais avec des partenariats très forts entre civils et défense : avez-vous un avis sur ce centre ?

M. Philippe Michel-Kleisbauer. Auditeur de la session cyber de l'Institut des hautes études de défense nationale, je faisais partie de l'équipe de *hack back* et nous nous sommes beaucoup posés de questions de droit international. Le manuel de Tallinn qui en est à sa deuxième édition, neuf ans après la première, pose des principes de « *due diligence* », de souveraineté, de caractérisation. Nous sommes sur un modèle différent des Anglosaxons, des *Five Eyes* (FVEY), qui détectent, remédient et font du *hack back* avec les services secrets. Vous disposez de cette capacité de *hack back* quand il s'agit d'une attaque militaire ou de défense jugée comme telle, dans la chaîne de commandement avec le Président de la République à sa tête, mais c'est à l'ANSSI qu'il revient de porter remède quand il s'agit d'affaires purement civiles. Cette dichotomie peut d'ailleurs être intéressante pour nos entreprises parce qu'elle signifie que les services de renseignement ne mettent pas leur nez dans leurs affaires. Toutefois ce droit international de Tallinn est en train de se cristalliser, et un autre problème se pose avec l'intervention sur tous les théâtres d'opérations – dont le cyber – des sociétés militaires privées (SMP) ou des entreprises de services de sécurité et de défense (ESSD), c'est-à-dire des sociétés militaires privées. Si nous restons dans une culture du refus de ces SMP et du *hack back*, certaines de nos multinationales pourront, dans les pays où elles interviennent, tisser un lien avec une SMP pour faire du *hack back*. N'oublions pas que de grandes entreprises, très respectueuses de nos principes, comme Saint-Gobain ou Altran, ont subi de l'extérieur des attaques importantes. Allons-nous pouvoir continuer à faire respecter notre propre droit sur nos propres pistes ou devra-t-on entrer dans cette mêlée plus anglosaxonne qu'est le manuel de Tallinn, à l'élaboration duquel aucun Français n'a jamais été convié ?

M. Jean-Charles Larsonneur. Je souhaite à mon tour évoquer les spécificités de la cyberdéfense dans le domaine naval. Des plateformes comme les FREMM doivent être mises à niveau et d'autres, comme les frégates de défense et d'intervention (FDI) sont déjà mieux équipées. Avez-vous quelques réflexions sur ce sujet ? Je rejoins aussi la question relative à vos attentes à l'égard du nouveau centre national de cybersécurité maritime.

Ma seconde question porte sur nos liens avec : où en est notre coopération, tout au moins notre dialogue, avec les Britanniques ? Pourrions-nous aller plus loin dans le cadre de Lancaster House ?

M. Jean Lassalle. Compte tenu des enjeux majeurs que revêt aujourd'hui ce nouvel espace, ne faudrait-il pas créer la quatrième arme dont quelques-uns d'entre nous ont déjà

parlé, et la confier à l'armée ? Quitte à être observé et suivi, si je suis un important chef d'entreprise français, je préfère tout de même que ce soit par l'armée de mon pays que par des forces beaucoup moins amicales… En tout cas, on ne pourra pas continuer à se laisser percer comme nous le faisons, notamment presque systématiquement dans le domaine de la recherche.

M. Bastien Lachaud. Votre prédécesseur a souhaité renforcer le rôle de la réserve citoyenne cyber, et je voudrais savoir où vous en êtes de ce processus.

Ma deuxième question concerne le choix qui a été fait, en France, d'une responsabilité fonctionnelle du COMCYBER sur des unités qui dépendent des différentes armées. D'autres armées dans le monde ont fait un choix inverse, c'est-à-dire de disposer d'unités qui dépendent directement de leur COMCYBER qu'il projette en fonction des besoins : c'est le cas notamment des Australiens ou des Chinois. Où en sommes-nous de l'analyse de ce choix ? Confirmons-nous que nous avons fait le bon ou regardons-nous ces modèles pour voir si nous devons nous adapter ?

Général Didier Tisseyre. Nous ne recrutons pas en effet que des savoir-faire mais aussi des savoir-être, pour être sûrs que le loup n'entre pas dans la bergerie. On peut ainsi imaginer des questions spécifiques lorsque l'on recrute des hackers parce qu'ils sont les plus performants. Nous sommes extrêmement attentifs. Des enquêtes sont menées, des contacts sont pris, des tests sont effectués et les recrutés ne sont pas tout de suite au cœur des opérations. Les faire commencer doucement nous permet de mieux les connaître. Ces personnes sont suivies de manière très précise pour qu'il n'y ait pas de difficultés.

Effectivement, plusieurs choix sont possibles en termes d'organisation au sens large. On peut regrouper l'ensemble des entités dans un seul service, sous un seul commandement : c'est le choix qu'ont fait certains États. Nous sommes plutôt sur un principe de modularité, de chaînes avec une coordination. Ainsi le commandement de la cyberdéfense est une petite entité avec un état-major inséré au sein de l'État-major des armées et des unités propres que nous sommes en train de regrouper sur la plaque rennaise pour qu'elles soient vraiment le « cœur du cœur ». Mais nous nous appuyons sur des chaînes d'armées, parce que les armées connaissent les systèmes qu'elles ont numérisés et sont en première ligne pour les défendre ou les protéger. Parce qu'on peut avoir à faire face à une attaque globale, il faut évidemment qu'on ait la connaissance de tout : mon rôle en tant que COMCYBER est d'orienter, de cadencer et de conduire l'ensemble de la défense du système, mais je m'appuie sur les chaînes d'armées, les chaînes de lutte informatique défensive d'armées – direction et services – qui sont au cœur de leur propre système. Nous sommes donc une structure relativement légère, qui n'a que les spécialistes les plus pointus, ou les plus « interarmées ».

Nous avons avec les organismes à vocation interarmées des contrats opérationnels, que nous revoyons régulièrement pour nous assurer qu'ils nous apportent les éléments de réponses escomptés.

La question s'est posée notamment par rapport à ce qu'on appelle la supervision de sécurité déployée sur les théâtres d'opérations. Le commandement de la cyberdéfense a des entités actuellement statiques, mais capables d'intervenir en fonction des incidents. Sur les théâtres d'opérations, nous nous appuyons sur l'armée de Terre et cette solution répond à nos besoins. Mais nous sommes assez attentifs. Le principe est de ne pas regrouper tout le monde et que des entités se retrouvent sans cybercombattants, sans cyberdéfenseurs. Est-ce le bon ? Cela nous amène à la question sur cette fameuse quatrième armée.

Ce qui est essentiel, c'est que le dialogue soit bon entre les divers services qui doivent travailler à la cyberdéfense. Celui qui est en charge de la défense doit être en contact étroit avec celui qui a conçu le système, et il faut des liens avec les autres opérations. Que tout le

monde soit en relation est d'ailleurs un peu un principe du cyberespace ; ainsi les frontières sont peut-être plus artificielles.

Ensuite, il faut définir une cohérence d'ensemble, avec un commandant de la cyberdéfense rattaché directement au chef d'État-major des armées, et ayant une place dans le périmètre ministériel, en tant que conseiller de la ministre. Un regroupement n'est pas obligatoire, quand bien même la question de l'information devient essentielle quand on entre dans une conflictualité d'une autre nature et non plus limitée aux espaces aériens, terrestre, maritime et spatial.

Peut-être faut-il aller encore plus loin dans l'appréhension et la gouvernance globales des systèmes, en associant davantage ceux qui conçoivent les systèmes et ceux qui les défendent.

Le domaine naval est très spécifique puisqu'on trouve dans une FREMM un système de systèmes. Il faut le prendre en compte dans la cyberdéfense, tout comme la fragilité ou de spécificité d'un lien satellitaire ou par ondes et non par câble. C'est pourquoi les marins sont les plus à même de comprendre les vulnérabilités et d'apprécier les possibilités du cyber. Pour autant, il faut une cohérence d'ensemble : c'est le CYBERCOM qui définit, planifie et conduit les actions offensives. Les marins ne sont donc ni autonomes ni livrés à eux-mêmes : nous dialoguons beaucoup et je suis là pour m'assurer que ça se passe bien. C'est le cas pour le centre maritime de cybersécurité, qui relève bien de la marine et qui est partie prenante de la chaîne de cyberdéfense.

Nos contacts avec le Royaume-Uni sont bons. Nous discutons beaucoup et travaillons ensemble au sein de la coalition contre Daech. Des progrès restent à faire, pour que les coopérations donnent des résultats concrets, mais ces partenariats entre entités spécialisées dans la cyberdéfense et le renseignement sont indispensables. Il faut surtout que nous nous appuyons sur des communications sécurisées : si les signatures de *malware* relèvent d'un niveau de classification intermédiaire, comprendre comment on a trouvé ces éléments et qui a été attaqué est très sensible et la transmisison de l'information doit se faire à un niveau de confidentialité qui dépasse le niveau secret.

Les réserves sont essentielles. Nous avons une réserve opérationnelle, avec des gens en uniforme qui travaillent au sein de nos unités à des actions de cyberdéfense au quotidien. Nous disposons aussi de réservistes citoyens qui nous apportent des expertises technologiques, sociologiques, par exemple par un échange dans des mécanismes de recherche.

M. Jacques Marilossian. Dans le rapport de septembre 2019 intitulé « Droit international appliqué aux opérations dans le cyberespace », le ministère des armées précisait les modalités de qualification d'une cyberattaque. Je cite : « cette décision est de nature régalienne en ce que la France se réserve le droit d'attribuer, publiquement ou non, une cyberattaque dont elle aurait été victime et de porter cette information à la connaissance de la population d'États tiers ou de la communauté internationale. Parallèlement, notre pays s'est engagé pour plus de régulation d'intelligibilité du cyberespace dans le droit international. Notre défi est donc de réussir le grand écart entre le maintien de nos moyens pour garder notre souveraineté intacte et aussi empêcher l'avènement d'une guerre toujours plus hybride aux contours très flous ». J'ai deux questions simples : pouvons-nous mieux définir, à partir de critères objectifs, ces différents types de cyberattaques ? Ou l'approche actuelle est-elle suffisante si nous voulons conserver une certaine lisibilité vis-à-vis du droit international ?

Mme Sabine Thillaye. Avec le *Cybersecurity Act*, l'Union européenne a adopté une posture un peu plus proactive que dans les années passées et l'on voit qu'il faut absolument se diriger vers une réponse concertée aux cyberattaques. Quelles sont vos relations avec l'ENISA (Agence de l'Union européenne pour la cybersécurité) ? Comment, dans le cadre qui

a été récemment défini, travaillez-vous ensemble ? Et comment les mesures restrictives qui sont aujourd'hui possibles vont-elles être véritablement mises en place ?

Ma deuxième question concerne plutôt l'ANSSI, qui met très souvent en garde contre les risques d'une succession d'attaques contre des intérêts français majeurs. Quels sont les moyens à notre disposition contre ce type d'attaques, si une activité économique est bloquée ? Comment peut-on mieux réagir aussi par rapport aux opérateurs d'importance vitale (OIV) qui, d'après le directeur de l'ANSSI, ne respecteraient pas les règles de précaution ?

M. Jean-Louis Thieriot. L'histoire militaire montre que des technologies de rupture ont eu des effets stratégiques majeurs, je pense au rôle du radar dans la bataille d'Angleterre. Y a-t-il aujourd'hui dans l'espace cyber des technologies absolument discriminantes qui nous permettent d'être ou non, au niveau de la menace ? Si oui, les possédons-nous ? Avons-nous les moyens de les posséder face aux acteurs majeurs que sont les Russes, les Chinois et, bien évidemment, les États-Unis ? En clair, y a-t-il un problème de moyens technologiques pour être à la hauteur ?

M. Philippe Folliot. En cyber, c'est comme au rugby : la meilleure défense c'est l'attaque. Aussi, je voudrais savoir quelle est la part des moyens humains, matériels et autres que vous pouvez consacrer à nos capacités offensives. Vous l'avez dit à mots à peine couverts, c'est un élément important et nous sommes dans une stratégie qui est du reste complètement à l'opposé de celle du feu nucléaire, dont la non-utilisation souhaitable et souhaitée.

Ma deuxième question a trait à la réserve opérationnelle. Combien de personnes sont concernées ? Ne pourrait-on par ce biais recruter les génies de l'informatique ? C'est ce que commencent à faire vos collègues des forces spatiales qui recrutent des personnels du CNES (Centre national d'études spatiales) qui peuvent jouer un rôle civil et, à un moment de la journée ou à un moment de l'année, prendre via la réserve une fonction militaire directement opérationnelle.

Ma dernière question porte sur la nature de nos liens avec nos partenaires de l'OTAN. Nous sommes censés aller tous dans le même sens, mais certains de nos grands alliés ont parfois des visions un peu différentes de la nôtre. Quelle est votre analyse ?

M. Loïc Kervran. Nous avons beaucoup parlé de cette menace relativement sophistiquée qui est le fait d'États-puissance, y compris par le truchement d'autres groupes. Mais existe-t-il un terrorisme cyber ? Le cyber est-il aussi l'arme du pauvre ou l'arme du riche groupe terroriste qui peut acquérir des capacités cyber ?

Et puis une question simple pour bien éclairer la représentation nationale : du fait de votre expérience opérationnelle, vous avez un sens aigu du danger. Pourriez-vous nous dire, dans tout le spectre de la menace étatique, terroriste, etc., et au regard de notre propre capacité, si la France est en cyberdanger ?

M. Nicolas Meizonnet. Vous avez évoqué la possibilité de neutraliser totalement certains systèmes, certains équipements et pris l'exemple des F-15 américains qu'on pouvait clouer littéralement au sol. À ce jour, y a-t-il des bâtiments, des infrastructures, des équipements français qui pourraient être neutralisés intégralement par une cyberattaque, c'est-à-dire non utilisables de façon déconnectée, mécanique, manuelle ? Je pense notamment à nos aéronefs de combat ou de transport, nos navires de surface, sous-marins, nos véhicules terrestres etc.

Je souhaiterais également savoir si nous pouvons nous considérer comme techniquement indépendants en matière de cybersécurité. Utilisons-nous des technologies étrangères ? Et, si c'était le cas, cela augmenterait-il nos risques de vulnérabilité ?

Mme Laurence Trastour-Isnart. On a évoqué la fragilité de nos moyens de communication satellitaires. Le système satellitaire est plus particulièrement vulnérable lors des cycles de renouvellement des satellites déjà déployés. Ces opérations dépendent des

entreprises civiles dont les satellites commerciaux sont ceux dont nos bandes passantes dépendent parfois également. Quels moyens sont déployés pour remédier à ces failles sécuritaires et quelles sont les solutions envisagées afin de maintenir la sécurité des communications satellitaires lors des renouvellements ?

Mme Sereine Mauborgne. Nous sommes un certain nombre au sein de cette commission à être membres du CyberCercle qui réfléchit à ces sujets de façon peut-être plus collective.

Ma question a trait aux systèmes d'armement. L'an dernier, lorsque les FREMM avaient été déployées près de la Libye, on s'est interrogé sur les capacités d'armement de la FREMM. Est-ce un type de cyberattaques qui serait envisageable et potentiellement réalisable ?

Général Didier Tisseyre. Dans un rapport tel que celui de septembre 2019, ce qui est important, c'est d'être assez clair sur ce que l'on est capable de faire, sans définir trop précisément les seuils. L'ennemi, et surtout l'ennemi étatique, va regarder jusqu'où il peut aller et s'il comprend qu'il peut avoir un certain impact en restant au-dessous d'un certain seuil, il procédera de cette manière.

En revanche, il faut que soient bien définies les possibilités de défense, de riposte, qui sont offertes, avec une palette d'effets très large. Notre capacité de détection et notre veille sont aux niveaux les plus fins : s'il se passe la moindre chose, il faut qu'on soit capable de s'en rendre compte. C'est ensuite que l'on décide ce que l'on fait, en fonction du seuil, de la nature de l'attaque, etc. Le contenu de ce rapport est suffisant pour avoir un positionnement assez précis tout en ne portant pas trop d'éléments sur ces seuils à la connaissance d'un attaquant.

À l'inverse de l'OTAN, l'Union européenne est un peu plus tournée vers la cybersécurité et un peu moins vers la cyberdéfense militaire. C'est donc plutôt l'ANSSI qui est sa première interlocutrice. Mais nous nous tenons bien sûr au courant de ce que peut faire l'ENISA pour le développement de capacités dans un cadre OTAN et avec certains budgets. Il y a un côté dual cybersécurité/cyberdéfense militaire et on peut retrouver des mécanismes similaires. En tant que COMCYBER, nous nous sommes positionnés comme observateur dans un certain nombre de groupes de travail ou de groupes de développement des capacités en matière de cyberdéfense et cybersécurité. Bien évidemment, nous sommes plus présents encore dans les opérations et les structures de commandement de l'Union européenne, l'État-major de l'Union européenne, etc.

En ce qui concerne la menace pour la France, celle d'un *Pearl Harbour* est possible, évidemment. C'est ce que répète régulièrement Guillaume Poupard, directeur général de l'ANSSI. C'est envisageable parce qu'on découvre un certain nombre de logiciels prépositionnés, et parce que notre maturité technologique nous permet de mieux découvrir et mieux comprendre ces bouts de code qui étaient passés en dessous des radars. Nos radars sont désormais plus puissants, plus performants. Il faut faire en sorte que l'ensemble des entités, y compris les opérateurs d'importance vitale, soient plus ouverts à ces questions, comprennent mieux ces éléments. La loi permet à l'ANSSI de positionner des sondes chez ces opérateurs, mais aussi de créer des contacts pour pouvoir mieux connaître, mieux partager, et bénéficier davantage des éléments que peut apporter l'ANSSI. On est entré dans une dynamique d'ouverture, de compréhension, de la part de tout le monde. La réticence, la peur de se faire taper sur les doigts parce qu'on n'est pas au niveau, diminuent, même si nous devons poursuivre nos efforts de pédagogie. L'ANSSI en fait beaucoup. Mais le principe est d'éviter ce *Pearl Harbour*, d'éviter qu'un jour on se réveille dans la difficulté. Pour cela, nous devons en particulier faire comprendre aux OIV qu'il faut avancer dans ce domaine.

S'agissant des technologies qui peuvent se révéler destructives, l'IA est un bon exemple car elle peut permettre de faire énormément de choses, mais on peut aussi penser à la

combinaison de plusieurs technologies. En matière de détection par exemple, on utilisait beaucoup les détections périmétriques, sur les flux entrants et sortants, en y cherchant des *malwares*. Mais on a compris qu'il est aussi important d'aller carrément sur les postes de travail voir ce qui s'y passe ; d'aller dans les serveurs où il y a les données ; d'aller dans les serveurs où il y a les applicatifs. Il est important d'avoir une vision plus globale des systèmes pour voir quel est le comportement normal d'un système d'information. L'IA va précisément nous permettre de caractériser un comportement normal et de pointer un comportement qui ne l'est pas. Cette aptitude à intégrer diverses technologies est essentielle, d'où l'importance de disposer d'équipes pluridisciplinaires.

En 2017, le ministère des armées a subi environ 700 tentatives d'attaque. il s'agissait de cybercriminalité dans 90 % des cas et nous n'étions donc pas ciblés. Dans les 10 % restants, nous étions ciblés par un groupe élaboré, évolué. En 2018, on a compté environ 830 événements, avec ces mêmes pourcentages. En 2019, le total est monté à 850 mais on ne voit pratiquement plus d'attaques de groupes très élaborés, avec des signatures caractéristiques.

La première réaction est de se réjouir qu'on ne nous attaque plus parce qu'on sait que nous sommes bien protégés. La deuxième peut être de penser que nos attaquants sont en train d'utiliser des outils beaucoup plus discrets, ou qu'ils utilisent des outils de cybercriminalité pour nous induire en erreur alors qu'ils ont une stratégie d'action cachée. Ces constatations sont alignées avec celles de l'ANSSI ou d'autres services de renseignements. Peut-être parce que certains ont été pointés du doigt ou parce qu'on a publié beaucoup sur la connaissance des modes opératoires de tel et tel groupe rattaché potentiellement à des acteurs étatiques, les attaquants sont aujourd'hui de plus en plus discrets ; les attaques sont de plus en plus sophistiquées et on les voit moins. Il faut donc être encore plus vigilant.

Je parlais de groupes élaborés, mais qu'en est-il des attaques dites « du pauvre » ? Il y a en effet un risque car on trouve aujourd'hui relativement facilement sur le *dark web* des outils prépackagés qui permettent de mener un certain nombre d'attaques pour quelques dizaines ou quelques centaines de milliers d'euros. Dans la société en général, ce sont souvent des rançongiciels : il est assez facile finalement de bloquer un système car malheureusement tout le monde ne sauvegarde pas ces données et n'est pas capable de restaurer ses équipements rapidement. Les attaquants jouent sur ce manque de prévoyance et, au bout du compte, certains préfèrent payer la rançon plutôt que la reconstruction onéreuse de leur système. Le coût des attaques de type *WannaCry* et *NotPetya* se chiffre en centaines de millions d'euros alors que les mener n'a sans doute coûté qu'1 million d'euros, pas plus.

Vous m'avez demandé ce qu'il en était de notre souveraineté, notre indépendance, notre autonomie nationale. L'autonomie stratégique nationale coûte cher. Nous sommes autonomes sur le plan du chiffrement, par exemple. Ce sont des chiffreurs français, avec des composants français, toute une procédure française, et cela a un coût. Cette cyberprotection régalienne, c'est la moitié des investissements budgétaires en matière de cyber au sens large.

Se pose la question de l'équilibre entre le risque d'utiliser des technologies développées par d'autres pays et le niveau de sécurité que l'on souhaite avoir. On n'aura jamais une sécurité à 100 %. Pour le plus essentiel, le plus régalien – je pense au nucléaire, au chiffrement des données – il faut engager les budgets dont on a besoin pour être assuré du plus haut niveau de souveraineté et de robustesse. Pour le reste, il faut analyser le niveau de risque consenti. Si c'est uniquement pour *« surfer »* sur internet, il n'y a pas forcément besoin d'avoir des équipements hypersophistiqués. Ils peuvent être achetés un peu n'importe où, à partir du moment où l'on instaure des mécanismes de supervision. C'est là aussi une approche globale : il ne faut pas voir un équipement en particulier, même si cet équipement peut présenter un niveau de risque potentiellement élevé.

La question des satellites est très sensible, car évidemment une fois que le satellite est parti, il peut être parti avec des vulnérabilités et des *malwares* à l'intérieur. Ce sont des mécanismes très précis et très pointus de contrôle, et de contrôle étatique. Si c'est le ministère des armées qui commande un satellite, on adopte bien sûr des procédures très strictes, au travers de la DGA, de la DRSD (Direction du renseignement et de la sécurité de la Défense), du commandement de la cyberdéfense. Il s'agit d'aller voir, d'aider à comprendre le réseau et les mécanismes de sécurité, d'ouvrir un peu plus les portes pour avoir un meilleur contrôle, sur l'ensemble de la chaîne : les systèmes d'information pour la conception, les systèmes eux-mêmes, et ainsi suite… On s'est renforcé encore et encore dans ce secteur, en raison précisément de la vulnérabilité de ces systèmes.

Il faut aujourd'hui se mettre dans une posture d'utilisation maximale des possibilités pour garantir la supériorité opérationnelle de nos forces déployées en opération. À partir du moment où un moyen naval, aérien, terrestre est déployé à proximité d'un théâtre d'opérations, on pense de plus en plus à ce qu'il soit un relais, un relais cyber, un relais d'opérations cyber, au même titre qu'il faut bien évidemment intégrer – et de plus en plus – sa propre défense parce qu'il va être amené à croiser dans les eaux internationales, près de certaines côtes. D'autres savent que nos systèmes sont numérisés, interconnectés avec la métropole. Il y a donc des portes d'entrée qu'ils peuvent essayer de franchir pour pénétrer dans le système. Cela entraîne une montée en gamme, à la fois défensive et offensive, par rapport à l'action militaire que l'on souhaite mener.

En termes de ressources humaines, on peut considérer que deux cinquièmes de nos effectifs se consacrent à l'offensif et trois cinquièmes au défensif. Ce rapport sera certainement amené à évoluer. Peut-être que dans quelques années, avec la maturité de nos capacités offensives et les mises à disposition par chaque armée, pour soutenir leurs manœuvres, de capacités offensives, le rapport s'inversera. L'offensif, c'est ce qui attire le plus, mais le défensif est plus fort et réunit les vrais experts dans un périmètre plus large. Bien sûr, ils doivent connaître l'offensif pour faire du défensif mais il ne faut surtout pas lever le pied sur la défense : si une attaque systémique ennemie passe, tous nos systèmes seront bloqués. On ne doit jamais négliger le défensif, la protection, qui est une sorte d'hygiène de base.

Quelques chiffres à propos de la réserve opérationnelle. Nous avons un objectif de 400 réservistes opérationnels, répartis dans nos unités pour qu'ils puissent y travailler au quotidien et où ils passent en moyenne une trentaine de jours par an. Nous avons atteint à peu près la moitié de notre objectif. Ces réservistes opérationnels nous apportent leur expertise et une vision différente, à tel point que nous les utilisons par exemple dans le cadre de *Bug Bounty*, donc de tentatives de pénétration de système, sur des systèmes de sites internet des armées. Ces opérationnels que l'on connaît bien tentent de pénétrer ces systèmes – donc dans un cadre clairement défini – pour nous aider à renforcer leur robustesse, en complément d'équipes dont nous disposons en propre pour mener ces audits.

L'OTAN doit bien évidemment assurer sa cyberdéfense, c'est essentiel par rapport à ses propres structures de commandement et à ce qui est déployé sur les théâtres d'opérations. Mais elle doit aussi intégrer le cyber offensif. Cela se fait non par un développement en propre de capacités offensives de l'OTAN mais au travers de la mise à disposition par des nations de ce qu'on appelle des « effets souverains », c'est-à-dire de capacités offensives qui, parce qu'il s'agit d'un domaine sensible, sont maintenues et gardées par les nations, n'entrent pas dans une mise à disposition de la totalité des connaissances.

Mme la présidente Françoise Dumas. En tant qu'élus, la prise de conscience des enjeux de cyberdéfense fait partie aussi de nos responsabilités. Nous devons être davantage conscients des risques que nous prenons, y compris dans l'utilisation de nos moyens de

communication, de nos téléphones, de nos ordinateurs. Nous avons encore beaucoup de maturité à acquérir. Mais nous sommes à vos côtés. Merci, général, pour ces éléments très précieux dans notre réflexion.

*

* *

La séance est levée à onze heures quinze.

*

* *

Membres présents ou excusés

Présents. - M. Jean-Philippe Ardouin, M. Stéphane Baudu, M. Olivier Becht, M. Christophe Blanchet, Mme Aude Bono-Vandorme, M. Philippe Chalumeau, M. Jean-Pierre Cubertafon, Mme Jacqueline Dubois, Mme Marianne Dubois, Mme Françoise Dumas, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Philippe Folliot, Mme Pascale Fontenel-Personne, Mme Séverine Gipson, M. Loïc Kervran, Mme Anissa Khedher, M. Bastien Lachaud, M. Fabien Lainé, M. Jean-Charles Larsonneur, M. Jean Lassalle, M. Didier Le Gac, M. Christophe Lejeune, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Nicolas Meizonnet, M. Philippe Michel-Kleisbauer, Mme Florence Morlighem, M. Jean-François Parigi, M. Thierry Solère, M. Jean-Louis Thiériot, Mme Sabine Thillaye, Mme Laurence Trastour-Isnart, Mme Alexandra Valetta Ardisson, M. Pierre Venteau, M. Charles de la Verpillière

Excusés. - M. Xavier Batut, M. Sylvain Brial, M. Luc Carvounas, M. André Chassaigne, M. Olivier Faure, M. Richard Ferrand, M. Claude de Ganay, M. Thomas Gassilloud, M. Fabien Gouttefarde, M. Benjamin Griveaux, M. Stanislas Guerini, M. Christian Jacob, Mme Manuéla Kéclard-Mondésir, M. Jean-Christophe Lagarde, M. Gilles Le Gendre, M. Franck Marlin, Mme Monica Michel, Mme Josy Poueyto, Mme Natalia Pouzyreff, M. Joaquim Pueyo, M. Joachim Son-Forget, M. Stéphane Trompille, M. Patrice Verchère