ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

# Compte rendu

## Commission de la défense nationale et des forces armées



Mercredi
21 février 2018
Séance de 11 heures

Compte rendu n° 36

SESSION ORDINAIRE DE **2017-2018**

**Présidence de M. Jean-Jacques Bridey,** *président*

ASSEMBLÉE NATIONALE

*La séance est ouverte à onze heures.*

**M. le président Jean-Jacques Bridey.** À la différence de notre réunion précédente, cette audition n'est pas ouverte à la presse – ni aux réseaux sociaux… Nous recevons Louis Gautier, secrétaire général de la défense et de la sécurité nationale (SGDSN), qui va nous parler principalement, mais peut-être pas uniquement, du volet cyberdéfense de la loi de programmation militaire, ainsi que de la revue stratégique de cyberdéfense.

**M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.** Merci pour votre accueil. Les travaux sur la revue stratégique de cyberdéfense, qui est d'ores et déjà accessible en ligne, et sur la loi de programmation militaire (LPM) ont été conduits dans le même cycle temporel. Le projet de LPM a été approuvé en conseil de défense juste avant la revue de cyberdéfense, et ces deux exercices ont été présentés en conseil des ministres le 8 février dernier. Il y a eu une concordance de temps, notamment dans la préparation interministérielle conduite par le secrétariat général de la défense et de la sécurité nationale (SGDSN), mais aussi un croisement entre les travaux puisque l'article 19 du projet de LPM est consacré à un dispositif intéressant notre cyberdéfense – c'est la reprise juridique des préconisations visant à renforcer la détection des incidents et des cyber-attaques.

Je ne reviendrai peut-être pas très longuement sur la LPM, car je crois que vous avez d'autres occasions de travailler sur ce sujet.

À périmètre constant, la mission « Défense » bénéficiera d'un effort budgétaire de 197,8 milliards d'euros entre 2019 et 2023, ce qui permettra une remise à niveau et une amélioration de la cohérence d'ensemble. Dans ses vœux, le président de la République a souligné le risque que ce soit un peu une loi « d'ingratitude » dans la mesure où une partie de l'effort consenti vise à corriger des déficits ou des défaillances, notamment dans la cohésion opérationnelle des moyens des armées, et où l'on répond à la nécessité d'améliorer la disponibilité des matériels. Néanmoins, le modèle retenu à l'issue des travaux interministériels met également l'accent sur la technologie et la création d'un contexte propice au développement de l'Europe de la défense.

C'est une loi de remise à niveau et de cohérence, je l'ai dit, mais aussi de sincérisation : au-delà des hausses de crédits, importantes, qui sont prévues chaque année en vue d'atteindre, à l'horizon 2025, l'objectif de 2 % du PIB allant à notre effort de défense, la LPM prévoit une meilleure prévision du financement des opérations extérieures (OPEX) directement à la charge du ministère des Armées, et une réduction des reports de charges, qui se sont accumulés ces dernières années et représentent, d'une certaine manière, autant de dettes pesant sur l'avenir.

Enfin, c'est une loi de programmation qui a pour caractéristique d'insister sur la problématique humaine : c'est le premier axe de cette LPM « à hauteur d'homme ». La condition des personnels était prise en compte par ailleurs, naturellement, mais c'est la première fois qu'elle est traitée comme un objectif de la programmation.

La LPM vise au renouvellement de certaines capacités, notamment là où il y a des impasses ou des difficultés liées au maintien en condition opérationnelle (MCO), ainsi que pour certains équipements faisant partie des plus usés – je pense en particulier aux blindés médians, aux patrouilleurs et aux ravitailleurs. Cet effort permettra de continuer à garantir

notre autonomie stratégique et de contribuer à une autonomie européenne qui reste à consolider. Autre aspect important, les crédits pour la recherche connaîtront une hausse progressive : afin de préparer l'avenir, ils passeront de 730 millions d'euros à plus d'un milliard à la fin de la période considérée.

Sauf si vous le souhaitez, je n'en dirai pas davantage pour le moment : je crois que vous réalisez par ailleurs beaucoup d'auditions sur la LPM.

Comme je l'ai indiqué, cette loi comporte un article relatif à la cybersécurité. C'est un point sur lequel nous nous sommes interrogés. Il y a historiquement une forme de continuité, puisque les premières dispositions concernant l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en particulier l'extension aux opérateurs d'importance vitale d'un certain nombre d'obligations dans le domaine cybernétique, ont été introduites dans la précédente loi de programmation militaire. Il y avait aussi des considérations liées à l'urgence : on cherchait un véhicule législatif. Une loi spécifique aurait pu être envisagée, car la revue de cyberdéfense comporte beaucoup de mesures appelées à avoir un prolongement, notamment dans le champ sociétal : on aurait donc pu proposer une sorte de grande loi couvrant à la fois la cyberdéfense de la Nation et celle de la société, mais on a privilégié la rapidité en utilisant la LPM comme véhicule législatif. L'urgence était de renforcer nos capacités de détection pour faire face à des attaques majeures. L'article 19 de la LPM, qui concerne surtout la protection de l'État et des opérateurs d'importance vitale, a toute sa place dans les débats au sein de votre commission. D'autres développements pourront avoir lieu à la faveur d'autres textes, notamment dans le champ économique.

La revue de cyberdéfense a été élaborée à la demande du président de la République, dans le cadre d'un mandat confié au SGDSN par le Premier ministre à la fin du mois de juillet dernier. Les travaux, conduits pendant environ six mois, ont permis de très larges débats : plus de 200 personnalités ont directement apporté leur contribution ou ont été entendues. Nous avons notamment organisé plusieurs séminaires, dont l'un a été l'occasion d'échanger avec la Représentation nationale, en particulier vos rapporteurs en charge d'une mission d'information sur des sujets connexes. Des échanges importants ont également eu lieu au plan international : je me suis rendu à deux reprises aux États-Unis dans ce cadre, et nous avons beaucoup consulté nos partenaires britanniques et allemands, mais aussi australiens, japonais ou encore singapouriens....

Ces échanges ont permis de constater que la France accusait un certain retard en ce qui concerne la formalisation de sa politique de cyberdéfense. La présente revue est en quelque sorte le premier Livre blanc dans ce domaine : on peut faire une comparaison avec celui de 1972, qui a incorporé la dissuasion nucléaire dans la doctrine de défense française. Différents éléments existaient antérieurement – je pense en particulier aux essais nucléaires conduits à Reggane dans les années 1960 –, mais c'est en 1972, dans le cadre du premier Livre blanc, que l'incorporation doctrinale a eu lieu. De même, il y avait déjà des éléments concernant le domaine cybernétique dans les Livres blancs de la défense nationale de 2008 et de 2013, ainsi que dans la stratégie nationale pour la sécurité du numérique, élaborée par l'ANSSI en 2015, mais le modèle n'était pas consolidé et, surtout, la doctrine n'était pas définie. Cette revue stratégique inscrit dans le champ de la doctrine et dans celui des politiques publiques notre stratégie pour les aspects cyber, qui sont désormais une dimension de la conflictualité à prendre en compte.

Nous avions trois objectifs pour cette revue. Politiquement, il s'agissait d'assurer une mobilisation des responsables et de l'opinion sur ces questions. Sur le plan stratégique, l'idée était de stabiliser un modèle et une doctrine adéquate pour mieux nous défendre. Il y avait aussi une dimension pédagogique, qu'illustre notamment la première partie du document, consacrée à l'évaluation de la menace. On s'est aperçu, en effet, qu'il existe très peu de documents officiels dans ce domaine, que ce soit en France ou à l'étranger, en français ou en anglais : la description de la menace engage déjà, notamment en ce qui concerne les sources et l'attribution des attaques – mais je pourrai vous expliquer comment nous avons surmonté cette difficulté. Par ailleurs, on ne trouve même pas nécessairement des ouvrages académiques généraux qui permettraient de comprendre aisément la menace à laquelle nous sommes confrontés. La documentation existante est destinée à des experts et elle est alors très technique ou bien elle n'a pas d'une précision suffisante.

Nous avons en effet affaire à une aggravation de la menace, comme j'ai pu le constater très vite dès que j'ai été nommé, en 2014. Depuis, on assiste à la généralisation, l'intensification et la sophistication des attaques.

Ainsi internet est utilisé comme vecteur pour des trafics illicites, des fraudes ou des attaques beaucoup plus ciblées contre des intérêts publics et privés.

Les menaces sont de quatre types.

La plus commune et la plus simple, qui était déjà dans toutes les têtes il y a dix ans, est l'espionnage, la captation de données – par des États ou des acteurs industriels – à des fins concurrentielles ou de pillage de brevets, voire le « défacement » de sites.

La deuxième menace est la cybercriminalité. Avec le développement du *bitcoin* et des cryptomonnaies, on est face à un océan de trafics divers. À une économie noire, qui se chiffre en milliards de dollars, sous des formes allant des petits trafics à la vraie criminalité, dans le *dark web*, en passant par le financement d'acteurs qui peuvent être étatiques – lors de la dernière vague de « rançongiciels », on a ainsi pointé du doigt la Corée du Nord, qui était à la recherche de sommes importantes pour financer sa prolifération. Malgré toute l'attention dont la cybercriminalité doit faire l'objet, il y a très peu de moyens du côté de la justice, très peu de moyens spécialisés pour la police également, et une très grande difficulté à coopérer au plan international pour attribuer les faits et sanctionner les infractions.

La troisième menace est le sabotage. Avec le virus Stuxnet en Iran et l'exemple de la neutralisation de terminaux pétroliers, on a vu depuis plusieurs années qu'il est possible de causer des dégâts dans le monde physique par une prise de contrôle dans le cyberespace. Il n'est plus seulement question de provoquer des pannes informatiques ou des *black-out*, mais de s'infiltrer par exemple au moyen d'une simple clef USB, ou d'un accès à partir d'un système administratif, et de remonter ensuite jusqu'à des systèmes de sécurité, ce qui peut permettre de prendre la main, par exemple, si le dispositif est insuffisamment protégé sur l'ouverture des portes d'une ligne de métro automatique, un sas de sécurité, un circuit de signalisation routière. Il y a un réel danger dans des sociétés de plus en plus numérisées qui ont d'abord et avant tout utilisé l'informatique pour ses formidables potentialités d'échange et de mise en relation, sans que l'architecture des systèmes informatiques ait été pensée en intégrant d'emblée la question de la cybersécurité. Avec le développement des automates, de

l'intelligence artificielle et des objets connectés, cela doit impérativement être fait dès la conception de tels équipements.

La dernière évolution de la menace, qui est aujourd'hui relatée dans tous les journaux parce qu'elle se trouve au cœur de l'enquête menée aux États-Unis par le procureur spécial Robert Mueller, est la déstabilisation. En 2016, étant informé de ce qui se passait aux États-Unis, j'ai obtenu que l'on applique en France des méthodes permettant de mieux sécuriser la campagne présidentielle et les élections de 2017, de façon générale et, au-delà de la seule question du vote électronique, pour nos ressortissants à l'étranger.

Ce choix a suscité un certain nombre de questions, comme le savent bien les représentants des Français de l'étranger, mais nous avons pris cette décision au regard de l'évaluation du risque. En outre, devant la vague de propagande, de *fake news* et de référencement abusif de contrevérités à laquelle on assistait, j'ai demandé à l'ANSSI de réaliser une veille sur internet et, en cas d'attaque, ce qui est arrivé, de mettre les résultats à la disposition du président de la commission nationale de contrôle de la campagne électorale et du juge de l'élection, à savoir le Conseil constitutionnel. Un effort de pédagogie a par ailleurs été réalisé en direction des équipes des candidats, afin qu'elles soient davantage en mesure de faire face aux risques. L'ANSSI est intervenue à la demande de la commission de contrôle après une attaque contre l'équipe d'un candidat.

Cette dernière menace pose une vraie question dans nos démocraties. Alors que, dans le cas de la plupart des cyberattaques, pour les empêcher ou les contrer, l'on peut se limiter à une analyse des contenants et des données d'enveloppe des messages toxiques, il faut en l'occurrence, s'agissant des actions de déstabilisation, réaliser une analyse du contenu – celui des fausses nouvelles, par exemple –, ce qui constitue un sujet extrêmement difficile dans une démocratie.

Au-delà de la caractérisation des menaces par rapport à leur finalité, il faut aussi les distinguer selon leur caractère ciblé ou au contraire indiscriminé.

Dans le premier cas, les menaces émanent d'États ou d'organisations qui peuvent être liées à eux, notamment les groupes connus – depuis 2006 – sous le nom d'*advanced persistant threats* (APT). Des systèmes d'attaque et des logiciels malveillants extrêmement élaborés sont alors utilisés à des fins de pénétration et d'infiltration, souvent sur la longue durée. L'attaque subie par TV5 Monde a ainsi été préparée entre trois et quatre mois à l'avance. Les opérations qui ont touché l'Ukraine, notamment *NotPetya*, concernaient un logiciel utilisé par près de 80 % de l'administration, et dont une faille avait été détectée deux ou trois mois plus tôt. On n'a donc pas affaire à des *hackers* s'amusant depuis leur garage. Pour réaliser de telles opérations il faut avoir une capacité d'infiltration et de pénétration, savoir rester tapi dans les systèmes, clandestinement, afin de ne pas se faire détecter, et disposer des infrastructures nécessaires, notamment pour le commandement et le contrôle de l'attaque, mais aussi pour l'exploitation des milliers ou des centaines de milliers de données collectées, en vue d'extraire celles qui sont les plus pertinentes. Une telle sophistication n'est pas à la portée de n'importe qui.

Certaines menaces sont ciblées, alors que d'autres ont des effets indiscriminés, l'intention pouvant être, au demeurant, de produire un effet systémique. Des virus tels que les rançongiciels peuvent cibler un pays, à l'origine, mais échapper ensuite à leur inventeur, ce

qui produit des effets de bord – l'Ukraine est visée mais Saint-Gobain est également touché, par le biais d'une filiale ukrainienne. Il arrive que les virus échappent à tout contrôle, se multiplient et prolifèrent, ce qui provoque un effet « tsunami ».

La seconde partie de la revue stratégique est probablement celle qui vous concerne le plus directement, car elle est relative à la responsabilité de l'État dans l'organisation de la cyberdéfense de la Nation.

Cela nous a conduits, dans un premier temps, à définir un périmètre : le cœur, le cerveau et les fonctions vitales que l'on doit impérativement renforcer pour permettre à l'État de résister à un choc, de disposer de moyens de résilience si une partie des murailles s'est effondrée, et d'assurer la continuité d'un certain nombre de fonctions sans lesquelles on serait réduit à la passivité face à d'autres chocs, ayant d'autres origines, éventuellement de nature militaire. Ce périmètre inclut des systèmes informatiques relevant directement de l'État – au sein des armées et des services de sécurité ou de secours – mais également de services aussi essentiels que la distribution de l'énergie et les télécommunications. Le SGDSN et l'ANSSI ont considéré que l'on devait renforcer la main de l'État afin de protéger l'ensemble des fonctions essentielles et des infrastructures critiques ainsi définies.

L'étape suivante a été de préciser un modèle qui faisait jusque-là l'objet d'une simple approche empirique. Nous avons fait le choix, judicieux à mon avis, d'une cyberdéfense reposant sur deux piliers : d'une part, les services de renseignement et le commandement de la cyberdéfense (ComCyber), qui sont en charge du renseignement et des actions de riposte ou d'attaque, y compris par des actions clandestines, et, d'autre part, l'ANSSI, agence interministérielle qui n'appartient pas à la communauté du renseignement et dont la mission consiste à définir des systèmes de protection d'une manière assez large, puisqu'elle agit à la fois pour le compte de l'État et en lien avec un certain nombre d'opérateurs vitaux.

Dans le cas de TV5 Monde que j'ai évoqué tout à l'heure, pourrait-on accepter facilement qu'un service de renseignement intervienne au sein d'un média public, ou privé, faisant l'objet d'une attaque ? L'ANSSI est une agence technique neutre, n'exploitant en aucun cas les contenus – ce n'est pas un service de renseignement – mais s'intéressant aux contenants, ce qui lui a permis, mis à disposition de l'autorité de contrôle de la campagne présidentielle et du juge constitutionnel, de jouer sans difficulté son rôle dans la sécurisation de nos dernières élections. La problématique apparaît rétrospectivement plus compliquée aux États-Unis, où les moyens de cyberdéfense sont réunis au sein de la communauté du renseignement, dont la NSA spécifiquement en charge du domaine. Ce système bute sur des conflits de principes et des risques d'interférence : À quel moment l'attaque contre le Parti démocrate a-t-elle été détectée et « attribuée » ? Si les services de renseignement l'ont vue, pourquoi n'en ont-ils pas fait part aussitôt ? Mais pouvaient-ils le faire eux-mêmes sans saisine d'un juge dès lors que l'opération se déroulait sur le territoire américain ?

Je pense que notre propre système est vertueux : il assure un équilibre démocratique en distinguant bien les missions, et il favorise une très forte coopération avec les opérateurs en ce qui concerne la détection – j'y reviendrai. Certains de nos grands partenaires ont choisi le même modèle que le nôtre, notamment les Allemands, et nous pensons que ce choix devrait également prospérer ailleurs en Europe.

Sur la base de ce modèle, nous avons considéré qu'il était nécessaire de bien définir les chaînes opérationnelles et, surtout, de mieux les faire travailler ensemble.

La revue stratégique a ainsi distingué quatre chaînes : celle de la protection, qui est largement confiée à l'ANSSI, sous la responsabilité du SGDSN et du Premier ministre ; l'action militaire ou clandestine, qui relève du ComCyber et de la direction générale de la sécurité extérieure (DGSE), pour l'essentiel, et qui remonte jusqu'au président de la République, par exemple quand une opération extérieure est décidée ; l'action en matière de renseignement, notamment pour l'anticipation et l'attribution, qui implique les services spécialisés, en particulier la direction générale de la sécurité intérieure (DGSI) ; l'investigation judiciaire – j'ai rappelé tout à l'heure la nécessité de renforcer l'action de la justice contre la cybercriminalité.

En ce qui concerne la chaîne du renseignement, le travail de Robert Mueller aux États-Unis montre bien que l'attribution ne peut pas résulter d'un simple travail de police scientifique – celui que fait l'ANSSI dans notre pays. Quand elle intervient à TV5 Monde ou à Saint-Gobain, cette agence se concentre sur la « scène du crime » : elle décrit techniquement l'attaque avant de procéder à des remédiations. Le constat et le diagnostic sont transmis aux services de renseignement ou à la justice, s'il y a une enquête. Très souvent, la caractérisation technique ne permet pas une attribution : on a reconnu tel APT, telle signature informatique ressemble à ce que font les Russes, les Coréens du Nord ou le groupe de *hackers* Lazarus, mais on doit se méfier de tout le monde dans ce domaine. Nous n'avons pas vraiment d'alliés et les faux nez existent : on peut laisser derrière soi les traces de doigts des autres. Il faut donc un travail de renseignement, qui ne peut pas relever de l'ANSSI. Cela implique d'aller au contact et de réaliser, par exemple, des écoutes. On le voit bien dans ce que les journaux rapportent du travail réalisé par le *Federal Bureau of Investigations* (FBI) pour caractériser selon leurs conclusions l'origine russe des attaques qui ont été commises aux États-Unis. Nos services de renseignement étant placés sous une autorité ministérielle, ces investigations à fins d'attribution se placent dans le cadre de la loi de 2015 sur le renseignement et ne posent pas de problème de mise en œuvre.

La revue stratégique décrit ces quatre chaînes opérationnelles, en précisant que l'ensemble des missions – l'anticipation, la détection, l'attribution, la riposte ou la réaction et les contre-mesures – doivent être exercées dans le cadre d'une coopération entre tous les acteurs. Nos moyens ne sont pas à la hauteur de ceux des États-Unis, à savoir des milliards de dollars et des dizaines de milliers de personnes travaillant sur les questions de cybersécurité. Il n'y a pas non plus encore une équivalence de moyens avec ceux des Britanniques ni même avec ceux des Allemands. À titre d'exemple, l'ANSSI compte environ 550 agents, contre 800 pour le service équivalent en Allemagne, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI). C'est pourquoi il est absolument nécessaire d'assurer une très forte coopération entre tous les moyens réunis, notamment ceux du ministère des Armées et de l'ANSSI, dans une consolidation capacitaire prenant en compte les moyens de la direction générale de l'armement (DGA), DE la direction technique de la DGSE DU ComCyber, et de l'ANSSI.

C'est sur ce socle de compétences techniques, et notamment sur des fonctionnalités extrêmement importantes en termes de fabrication de sondes, d'outils de détection ou de chiffrement des données, que sont focalisés les moyens les plus importants.

La DGSI qui emploie une centaine de personnes, qui ne sont pas toutes ingénieurs spécialisés en cybersécurité, doit mieux trouver sa place dans cet écosystème notamment pour réaliser les attributions et prévenir la menace.

Le ComCyber monte en puissance, tandis que la majorité des moyens sont actuellement répartis en trois blocs de taille comparable à la DGA, à la DGSE ainsi qu'à l'ANSSI. Nous souhaitons consolider ce socle technologique.

La revue s'est ensuite interrogée sur la problématique de la doctrine. Certains d'entre vous m'avaient d'ailleurs interrogé : doit-on publier une doctrine ou faut-il conserver l'ambiguïté ? J'ai toujours eu le sentiment qu'un pays comme le nôtre devait disposer d'une doctrine, mais ne pas intégralement la dévoiler. En effet, d'une certaine manière, quand les États-Unis font de l'attribution, ils sont en situation de supériorité. Ils vont jusqu'au bout de leur logique. Ils peuvent parfois se tromper aussi. Quand bien même, ils agissent à des fins purement politiques. Mais la France trouve plus d'avantages à conserver cette flexibilité, cette plasticité dans ses réactions : il ne faut pas rigidifier nos réactions ni les automatiser dans une doctrine.

Pour autant – le parallèle avec la doctrine de la dissuasion se révèle ici partiellement pertinent –, nous devons pouvoir affirmer que nous allons nous défendre et que nous ne nous laissons pas faire. C'est d'ailleurs ce qui se passe : nous ne nous laissons pas faire, même si nous n'affichons pas nos réactions.

La revue dans sa version publique, même si elle ne les décrit pas par le menu, assume clairement une logique de riposte. À partir de l'établissement d'un schéma de classement des agressions qui figure dans ce document, nous avons consolidé des méthodes d'analyse et de réaction et avons établi des passerelles, comprenant des niveaux de définition des seuils d'agressivité d'attaque. Ces seuils sont cohérents avec ceux des Américains et nous permettent d'échanger avec nos grands partenaires. Il ne s'agit pas cependant d'une doctrine de dissuasion car, qui dit dissuasion, dit automaticité de la réponse et absence de doute sur la réplique en cas d'atteinte à nos intérêts vitaux ; et même s'il reste une ambiguïté sur la définition de l'intérêt vital et le moment où l'on considère qu'il est touché, la réplique est automatique dès ce constat.

Nous souhaitons au contraire maintenir de la réversibilité et de la graduation dans le domaine de la cyberdissuasion ; cela va d'une simple démarche diplomatique, confidentielle – il m'est ainsi arrivé d'indiquer à d'autres pays que nous avions détecté leurs agissements et qu'ils devaient cesser –, à l'action militaire – si l'on considère que l'article 51 de la Charte des Nations unies doit être actionné, pour des raisons de légitime défense. L'escalade est donc possible dans le domaine de la cybersécurité.

En outre, l'effet dissuasif n'est pas le même que dans le monde réel. Nous l'avons appelé « découragement » dans la revue : notre posture doit être ferme et faire comprendre à ceux qui voudraient s'en prendre à nous que, de toutes les façons, quel que soit le mode de réaction, il y aura une réaction qui fera qu'en fonction de son niveau, l'agression sera sanctionnée… Il s'agit, aussi, par l'affirmation de cette posture réactive, de décourager les attaques.

Cette deuxième partie de la Revue est au cœur des problématiques de votre commission de la Défense et de la réflexion sur l'organisation de l'État.

La troisième partie est aussi extrêmement intéressante, mais plutôt tournée vers l'État en tant que garant de la cybersécurité de la société. Elle appelle l'ensemble des acteurs à travailler conjointement, afin d'augmenter le niveau général de cybersécurité de notre pays. Seule la problématique de la souveraineté numérique vous intéresse directement dans cette partie. En effet, à la différence des Américains ou des Chinois, la France ne dispose pas de grands équipementiers. Nous sommes plus vulnérables. Nous n'avons pas non plus Google, Apple, Facebook, Amazon et Microsoft – les GAFAM –, donc moins de possibilités de coopération ou d'influence . C'est pour cela qu'il est essentiel que nous conservions certaines capacités technologiques indispensables à notre souveraineté – chiffrement, outils de détection et d'attaque de sondes, *etc*.

C'est également tout l'intérêt d'un *cloud* européen ou, au minimum, de grandes banques de données permettant de conserver et de protéger correctement les données de l'État. Ce dernier doit également conserver la compétence de définition de systèmes de communication étanches, sur lesquels certains équipementiers ne peuvent pas intervenir. Cela implique que nous conservions de grands acteurs en France, autour d'Orange, d'Atos, d'Airbus et de Thales – nous avons encore récemment perdu Alcatel… Autour de ce noyau, nous pourrons développer des opérateurs de standard européen, voire international, nous permettant de conserver des briques – ou des niches – essentielles, sans parler du rôle de toutes les start-up européennes innovantes.

Plutôt que de prolonger cette intervention, je pense qu'il est plus intéressant maintenant d'échanger avec vous. En conclusion, j'ajouterai que beaucoup d'évolutions vont passer par la mise à jour des normes professionnelles, les diligences comptables, l'évaluation et la notation des cyber-risques. Dès l'école, nous devons également sensibiliser davantage les Français à cette problématique. Vous trouverez ces éléments de politique publique décrits dans la revue stratégique.

Pour finir, j'en viens à l'article 19 du projet de loi sur lequel nous pourrons également échanger. Il prévoit une coopération entre l'ANSSI et les opérateurs de communications. Si l'on pense tout de suite aux grands – Orange, SFR, Free –, en réalité, une centaine d'acteurs – opérateurs ou hébergeurs – pourra mettre en place un système préventif sur ses flux de communication, afin de détecter des virus, des attaques ou de possibles incidents. L'ANSSI communiquera à ces opérateurs un certain nombre de signatures de logiciels malveillants ou de marqueurs d'attaque. Enfin, dans certains cas, l'ANSSI sera plus directive en orientant la « pêche ». Elle pourra demander aux opérateurs de réaliser certains tests et interviendra même directement s'agissant des flux de données des opérateurs d'importance vitale ou de l'État.

Le système initialement prévu par la loi de programmation militaire de 2014 prévoyait que l'ANSSI intervienne seulement sur les réseaux de l'État et des opérateurs d'importance vitale, éventuellement sur les branchements entre les réseaux de communication et ces opérateurs ou l'État, mais pas sur l'ensemble de ces flux de données, alors que, pourtant, les risques d'attaques, de *malwares* et de virus sont omniprésents. Avec les nouvelles dispositions de l'article 19, la détection des attaques sera à la fois plus complète et mieux anticipée.

**M. Philippe Chalumeau.** Je vous remercie de ce propos liminaire. Ma question porte sur notre sujet du moment : le projet de loi de programmation militaire. À l'horizon

2025, elle prévoit plus de mille équivalents temps plein (ETP), notamment dans tous les domaines cyber. Quel est votre avis sur ce point ? Quelles seront les missions de ces nouveaux arrivants ?

**M. Joaquim Pueyo.** Vous avez raison : dans les années à venir, le cyber sera un secteur essentiel. L'article 19 est-il suffisamment clair pour vous donner davantage les moyens de répondre à toutes sortes d'attaques ? Votre revue stratégique est intéressante. Vous évoquez longuement l'éducation des jeunes à la cybersécurité : cela ne pourrait-il pas être pris en compte dans le parcours citoyen obligatoire, qui pourrait être mis en place dans les collèges ?

**M. Louis Gautier.** Vous êtes taquin !

**M. Joaquim Pueyo.** Je parle sous le contrôle de Mme Dubois, qui a récemment rendu un rapport sur ce sujet. Je suis particulièrement sensible à cette problématique car, dans ma circonscription, pour différents motifs, un adolescent s'est suicidé suite à des menaces liées à la diffusion d'images… Ce sujet me paraît donc important, en dehors même des questions de sécurité qui touchent à la fois nos équipements d'armement et notre système général de sécurité.

**Mme Patricia Mirallès.** Les cyberattaques sont malheureusement de plus en plus fréquentes ; des États en sont parfois les auteurs. Le traité fondateur de l'Organisation du traité de l'Atlantique nord (OTAN) prévoit la solidarité de ses membres en cas d'attaques physiques ou matérielles de l'un d'entre eux. Mais qu'en est-il de la réaction de l'OTAN face aux cyberattaques, qui ne sont pas considérées et traitées de manière collective ?

**M. Claude de Ganay.** Les médias se complaisent à dire que nous sommes particulièrement vulnérables. A-t-on pu identifier les principales vulnérabilités de notre cyberdéfense ?

Ma seconde question sera un peu en marge de la LPM et concerne la refonte des niveaux de secrets de la défense nationale et la suppression du premier niveau – le « confidentiel défense ». N'est-il plus jugé pertinent ? Comment notre contrôle parlementaire va-t-il s'accommoder de cette suppression ?

**M. Olivier Becht.** Vous avez évoqué la vulnérabilité de nos infrastructures – notamment civiles – face aux bombes logiques, déposées dans leurs réseaux par certains de nos ennemis potentiels, voire par certains de nos alliés. De quels moyens de résilience – matériels par exemple – dispose-t-on en France ? Ainsi, les systèmes électriques des Chinois restent à l'heure actuelle majoritairement à commande manuelle, pour pallier toute défaillance numérique.

Vous nous avez également parlé de souveraineté numérique. Certes, nous n'avons pas de GAFAM, ni d'entreprises comme Baidu, Alibaba, Tencent et Xiaomi (BATX), mais ne sommes pas démunis en la matière. Ces GAFAM et BATX ont en partie prospéré grâce à la commande militaire. Quelle est notre stratégie au niveau européen ?

**M. Louis Gautier.** Monsieur Chalumeau, les mille emplois seront fléchés sur les trois pôles spécialisés du ministère des Armées : la DGA, le ComCyber et la DGSE. Par ailleurs, je pense que le ComCyber va évoluer et se densifier.

Toutes nos opérations militaires intègrent désormais cette problématique. Prendre le contrôle de l'espace aérien d'un pays implique de bombarder systématiquement les centres de défense anti-aérienne et les tours de contrôle des aéroports militaires. Il peut suffire de trouver des failles de sécurité, et avant même que notre adversaire l'ait compris, de mettre le pays à terre. Ces investissements répondent donc aux besoins du ministère des Armées – notamment à la nécessité d'intégrer les cyberattaques dans la problématique militaire – mais aussi à l'impératif d'auto-protection de nos moyens. Si des vulnérabilités existent chez les autres, nous devons éviter que nos propres équipements ne soient eux-mêmes exposés à des fragilités, au risque d'une possible neutralisation.

Nous avons essayé de trouver un bon équilibre concernant l'article 19. Il a été présenté au Conseil d'État, qui a approuvé le système. Le dispositif est, je le rappelle, sous le contrôle de l'Autorité de régulation des communications électroniques et des postes (ARCEP). Cela n'empêchera par ailleurs pas le débat et les discussions au Parlement.

Monsieur Pueyo, vous évoquiez cet adolescent d'Alençon qui s'est suicidé. Nous sommes confrontés à ces difficultés et à ces drames dès l'école et le collège. Nos concitoyens doivent avoir conscience qu'un manque de protection de leurs données les expose, leur vie entière. Dans le domaine public, cela nous renvoie en outre à notre responsabilité en matière de protection du dossier médical ou judiciaire. En effet, la dématérialisation des grands services publics, comme ceux de la justice et de la santé, essentiellement pensée pour favoriser l'échange, doit désormais prendre en compte cette problématique de sécurité des données personnelles.

Madame Mirallès, l'OTAN prévoit une réaction collective aux cyberattaques, telle celle qu'a connue l'Estonie en 2007. Mais elle ne prévoit pas de répliques pour tout le reste. Ce n'est de toute façon pas souhaitable, car il s'agit d'un domaine de souveraineté. Je ne vous ai par ailleurs pas fait état de tous les cas plus ou moins exotiques que nous avons eus à traiter – certains mettent très directement en cause l'indiscrétion d'alliés… Rappelez-vous, à la suite de certaines révélations, les prises de position diplomatiques françaises certes feutrées mais fermes à l'égard de notre partenaire américain, après qu'on l'a détecté – un peu trop régulièrement parfois – en train de visiter nos sites étatiques… Dans ce domaine, on ne départage pas facilement nos amis et nos ennemis, sauf lorsqu'il s'agit de nos intérêts de sécurité : nos alliés ne s'y attaquent pas. Ils ne provoquent pas d'accident ou ne déstabilisent pas nos élections. C'est tout l'intérêt de la gradation des réponses.

Monsieur de Ganay, je n'entrerai pas dans cette logique de l'invulnérabilité. Notre discussion est franche. Il est important de faire passer le message concernant la nature de la menace. Mais il ne s'agit pas non plus de créer des angoisses inutiles dans la population. Nous avons tout de même une longueur d'avance « dans la consolidation de la cuirasse » – dans toutes les formes de conflictualité, on retrouve cette dialectique de l'épée et de la cuirasse. En effet, il y a un certain temps, nous avons créé la catégorie des opérateurs d'importance vitale (OIV) pour des raisons de sécurité physique – protéger les centrales nucléaires et, plus largement, Électricité de France (EDF) ou la distribution de l'eau, ou les transports... Depuis la dernière loi de programmation de 2014, l'ANSSI peut imposer des obligations pour sécuriser les réseaux informatiques des OIV. Cela nous a donné une formidable avance sur nos partenaires européens, pour travailler avec ces opérateurs et renforcer leur cybersécurité.

Les autres pays européens ne pouvaient pas le faire. Ce n'est que maintenant qu'ils rattrapent ce retard, par le biais des dispositions prévues par la directive du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union – *Network and information security* (NIS). Ces dispositions européennes concernent des activités essentielles, mais elles n'ouvrent pas la possibilité d'audits, que l'ANSSI réalise déjà directement, imposant ensuite des remédiations immédiates. Nous disposons donc d'un énorme avantage… Beaucoup cependant reste à faire. L'actualisation des défenses des systèmes informatiques des systèmes de l'État ou des OIV est un travail permanent.

Vous avez raison, nous envisageons de réformer les niveaux de secrets de la défense nationale, par parallélisme avec les niveaux de secrets de nos alliés, en particulier anglo-saxons. Le SGDSN négocie des accords généraux de sécurité. L'an passé, j'en ai négocié un avec l'Australie pour protéger les échanges de données, notamment dans le cadre du contrat de vente de sous-marins. Ces négociations étaient jusqu'à présent toujours extrêmement compliquées : nous n'étions jamais au « bon étage » avec nos partenaires. Cette réforme permettra de remettre nos niveaux de secrets d'équerre avec ceux de nos partenaires, en prévoyant un niveau « secret de la défense et de la sécurité nationale » et un niveau « très secret ».

Par ailleurs, le rapport sur le secret de la défense nationale a souligné l'inflation de classification dans le bas de l'actuel « confidentiel défense » : des millions de données parfois sans importance ont été classifiées… Or, pour bien protéger le secret de la défense nationale, il ne faut pas faire de classifications inutiles. À l'avenir, le « secret » va reprendre uniquement la tranche haute du « confidentiel défense ». À ce niveau de secret va en outre correspondre une génération nouvelle de moyens électroniques, dématérialisés ou de communication – autour des outils existants que sont l'intranet sécurisé interministériel pour la synergie gouvernementale (ISIS), OSIRIS ou HORUS pour les visioconférences.

Le niveau « très secret » pourra quant à lui être décliné en « X secret », pour les dossiers les plus sensibles, liés à des enjeux de souveraineté, qui ne sont donc pas partagés avec nos alliés. C'est, par exemple, le cas de la dissuasion nucléaire.

Cette réforme va nous permettre de disposer d'un système plus homogène. Nous prendrons notre temps, afin que tout s'adapte convenablement. Par ailleurs, dans tous les codes, un travail légistique sera nécessaire. Pour autant, cela ne changera rien au passé, le « confidentiel défense » devenant « secret ». Nous n'allons pas tout reclassifier, cela n'aurait pas de sens ! Certes, la partie basse des documents d'ores et déjà classifiés « Confidentiel Défense » demeurera peut-être un peu trop protégée, mais la délégation parlementaire au renseignement ou les missions spécifiques de la commission de la Défense ne rencontreront pas, du fait de cette réforme, de difficultés particulières d'accès ou de conversion.

Monsieur Becht, vous avez raison concernant la résilience. L'exemple des élections est parlant. Comme le faisait remarquer le président du Conseil constitutionnel M. Fabius, il est parfois bon de s'appuyer sur des procédures physiques – de revenir à la préhistoire ! –, sauf à vouloir prendre des risques inconsidérés. Or, dans certains cas, on ne peut pas prendre ces risques, notamment quand il s'agit d'une élection : lorsqu'une urne est bourrée dans un bureau de vote, la commission se réunit, pondère, voire élimine les bulletins contestés pour le

bureau concerné. Mais un défaut dans un système informatique pollue l'intégralité du vote, en créant un effet d'insincérité sur l'ensemble du processus…

De la même façon, dans certains domaines de la sécurité, il faut mettre en place des systèmes hermétiques entre eux : ainsi, dans le domaine informatique, les services d'administration générale d'une centrale nucléaire ou d'un barrage hydraulique ne doivent pas pouvoir dialoguer avec les dispositifs de sécurité. C'est le B.A.-BA. Cela implique aussi des redondances et de l'étanchéité, afin d'assurer la résilience de ces équipements de sécurité.

**M. Gwendal Rouillard.** Depuis plusieurs mois, l'hypothèse d'une convention de l'ONU en matière de cybersécurité est évoquée, qui prévoirait par ailleurs un régime de sanctions. Quel est votre avis sur ce sujet ? S'il est positif, quelle peut être la place de la France dans ce dispositif ?

Nous parlons de plus en plus de systèmes de systèmes, d'architecture et de batailles des normes. Je pense notamment au futur système de combat aérien, mais pourrais prendre bien d'autres exemples. Dans quelle mesure le SGDSN peut-il participer à la définition de ces normes et de ces architectures ? C'est une bataille fondamentale !

**Mme Laurence Trastour-Isnart.** Je souhaite revenir sur la mise à contribution des opérateurs de télécommunications. Pouvez-vous nous expliquer comment cela va fonctionner, en prenant des exemples opérationnels ? Comment mettre en œuvre ces mesures sans que nos concitoyens ne nourrissent des craintes pour leur vie privée et pour la neutralité du Net ? Par ailleurs, comment les opérateurs de niches – étrangers – vont-ils être impliqués ?

**M. Bastien Lachaud.** Je vous remercie pour cette présentation de la revue de stratégie de cyberdéfense. Je ne reviendrai pas sur ces questions de cyberdéfense ; nous avons déjà échangé lors des travaux de la mission d'information. Je vous interrogerai sur la LPM et sur la compétence du SGDSN en matière de protection du secret de la défense nationale, mais également sur la réglementation interministérielle, en espérant que vous pourrez nous éclairer sur les articles 34, 38 et 41 du projet de loi, qui habilitent le Gouvernement à légiférer par ordonnance sur des sujets assez flous…

L'article 34 vise à créer une procédure unique bénéficiant des différentes dérogations existantes et à instituer, dans le cadre de cette procédure, des dérogations à l'obligation d'organiser une enquête publique pour instituer des servitudes d'utilité publique. L'article 38 vise quant à lui à déroger aux procédures d'installations classées pour la protection de l'environnement, afin de ne pas attendre la délivrance d'une nouvelle autorisation pour poursuivre l'exploitation des installations au-delà des capacités initialement fixées. Enfin, l'article 41 souhaite harmoniser les terminologies employées dans les codes de la défense et de la sécurité intérieure pour qualifier des matériels de guerre, armes, munitions et leurs éléments. Pourriez-vous nous éclairer sur ces dispositions ? Et, si vous n'êtes pas compétent, qui l'est ?

**M. Fabien Gouttefarde.** Ma question ne concerne pas directement la cyber mais un sujet de la compétence du SGDSN : les drones. Vous avez sûrement vu que l'ouverture des Jeux olympiques d'hiver en Corée du Sud nous a permis d'assister à un magnifique essaim de drones automatisés. Depuis quelques années, le SGDSN est à la manœuvre pour mettre en œuvre un système de défense contre des drones automatisés nuisibles. Quel est l'état d'avancement de vos travaux ? Ce système sera-t-il efficace ?

**M. Yannick Favennec Becot.** Avez-vous établi une liste hiérarchique – une forme de « hit-parade » – des acteurs, notamment étatiques, identifiés comme porteurs de menaces ? Si oui, pouvez-vous nous la communiquer ?

**M. Louis Gautier.** Monsieur Rouillard, nous sommes évidemment mobilisés, aux côtés de M. David Martinon, ambassadeur pour le numérique, dans la discussion de tout traité, accord ou convention qui permettrait de mieux réguler le cyberespace. Le SGDSN et l'ANSSI avaient d'ailleurs organisé à l'année dernière à l'UNESCO le colloque « La paix dans le cyberespace ». La France milite pour cette régulation, même si elle semble mal engagée pour le moment car le groupe d'experts gouvernementaux de l'ONU s'est dissous sans parvenir à conclure à la nécessité d'importer dans le domaine du numérique un certain nombre de normes applicables en droit international, sauf pour l'article 51 de la Charte des Nations unies sur la légitime défense que j'évoquais précédemment, qui s'applique dans le domaine cyber, tout comme l'ensemble de la Charte.

Les pays ont pendant longtemps travaillé de concert, avant que les Chinois et les Russes ne se désolidarisent, *in fine*. De gros efforts restent à fournir dans ce domaine, si l'on veut éviter que cet espace ne devienne le lieu d'une conflictualité systématique. Il ne faut pas oublier qu'à l'origine, c'est un formidable espace d'échange d'informations, de communication, de brassage culturel. Il faut veiller à ce que la multiplication du *hack back* – la vente d'outils agressifs que tout le monde utilisera en cas d'agression – n'aboutisse à une forme de Far-West numérique…

Monsieur Rouillard, vous évoquez également la bataille des normes. Le SGDSN prend des arrêtés et fixe des normes, en relation avec l'ANSSI. Cette dernière prend par ailleurs différentes dispositions impliquant des agréments et l'acceptation du développement de certains artefacts. Elle contrôle ce qui est vendu en France et valide des offres de confiance. Il s'agit donc déjà de normalisation. Mais vous avez raison, dans le domaine économique et surtout dans celui des normes industrielles, les Américains vont chercher à reproduire ce qu'ils ont réussi à imposer en matière comptable : les règles de conformité – *compliance* – qu'ils veulent nous faire adopter leur permettront de maîtriser encore mieux nos sociétés… Si les Européens ne s'empressent pas de fixer leurs propres normes professionnelles, ne créent pas leurs agences de notations du cyber-risque, n'impliquent pas des diligences comptables, le système sera déséquilibré…

Les Européens doivent donc produire de la norme, non pas seulement parce que c'est efficace en matière de cybersécurité, mais aussi afin d'éviter de se faire imposer par d'autres des normes ensuite possiblement détournées comme biais anticoncurrentiels.

S'agissant de la neutralité d'internet, Madame Trastour-Isnart, le système proposé à l'article 19 est avant tout coopératif. À preuve, le verbe employé dans le libellé de l'article : « les opérateurs de communications électroniques peuvent recourir… » ; autrement dit, ils ne le feront pas s'ils ne le veulent pas. Je crois cependant qu'ils rechercheront cette possibilité parce que l'article 19 vise non seulement à assurer la cyberdéfense de la Nation, mais il est aussi bénéfique pour tous les usagers et constitue un élément de la fiabilité des prestations et services fournis par les opérateurs. L'idée nous en est venue suite à un déplacement aux États-Unis, dont l'organisation diffère de la nôtre avec l'ANSSI. Pour imposer des formes d'obligation de ce type dans les contrats publics ou ailleurs, nous disaient nos interlocuteurs, il faut que les opérateurs s'y retrouvent ; pourquoi, dès lors, ne pas leur laisser la possibilité

de proposer des contrats de base – respectant la neutralité totale du réseau, en laissant notamment passer tous les virus et autres *spams* – et, moyennant deux euros supplémentaires, par exemple, des contrats aux termes desquels ils auraient la possibilité d'assurer une sorte de police sur la circulation sans toucher aux contenus mais seulement à la signature électronique, à l'enveloppe et aux métadonnées techniques des messages ?

En réalité, c'est un système coopératif entre les opérateurs de télécommunication et l'ANSSI qui leur fournira les signatures malveillantes complémentaires à celles que les acteurs privés peuvent également connaître car elles sont publiques. L'ANSSI ne prend pas directement la main en plaçant ses propres marqueurs ou ses sondes qu'en cas de risque d'attaque grave pour la sécurité de l'État ou celle des OIV. Ainsi, non seulement nous renforcerons notre système de détection mais aussi la prévention, puisque l'ANSSI informe régulièrement les opérateurs et entreprises des incidents repérés ou signalés. Si nous avons échappé à la première attaque du logiciel malveillant WannaCry qui a mis le système de santé britannique en panne, c'est sans doute grâce aux actualisations qui avaient été effectuées – parfois de manière très simple, grâce à des mots d'ordre et conseils donnés par l'ANSSI à l'ensemble de ses réseaux. À ceux qui s'interrogent, je dirai donc ceci : le fait que l'Agence soit impliquée aux côtés des opérateurs, que le dispositif ne touche en rien aux contenus mais seulement à des données techniques et que l'ARCEP soit autorité de contrôle, donne plus de garanties qu'aucun autre système. De surcroît, nul n'est contraint – sauf en cas de risque pesant sur la sécurité des systèmes de l'État et des opérateurs d'importance vitale.

Pour vous répondre, Monsieur Lachaud, il me faudra me pencher en détail sur les articles 33, 38 et 41 et sur les ordonnances. Le ministère des Armées vous fournira l'ensemble des informations et je suis prêt à regarder avec vous le détail technique de ces dispositions texte en main.

**M. le président.** Je précise que nous auditionnerons la directrice des affaires juridiques du ministère des Armées demain, à neuf heures, et que la question pourra lui être posée.

**M. Louis Gautier.** J'apprécie toujours les questions sur les drones, Monsieur Gouttefarde. C'est un sujet sur lequel la SGDSN et la représentation nationale ont produit un travail commun fructueux – qu'il s'agisse du colloque ou du rapport. La loi découle d'ailleurs d'une proposition d'origine parlementaire. Depuis, nous avons beaucoup évolué en instaurant des mécanismes de détection et de neutralisation des drones, notamment *via* des systèmes de brouillage et des canons à micro-ondes. Nous spécifions actuellement les projets de certains industriels.

La loi permet de discriminer : grâce au système d'immatriculation et au fichier, nous pouvons désormais identifier les drones qui ont une certaine portée et qui peuvent être agressifs car susceptibles de transporter, par exemple, des explosifs ; ils doivent être immatriculés et sont signalés par une balise. En étant ainsi en mesure de les repérer, nous pouvons donc discriminer, dans le flux de la circulation, les drones qui respectent la réglementation et les autres, que nous sommes incités à ne pas laisser approcher, en prenant des mesures préventives voire préemptives grâce aux moyens de détection et de neutralisation que j'évoquais. Ce n'est pas toujours aisé : les brouilleurs, par exemple, ne peuvent pas être utilisés à proximité d'un aéroport, ce qui oblige à utiliser d'autres types d'équipements comme les canons à micro-ondes. Nous allons donc articuler différentes technologies en

fonction de la zone à protéger. Quoi qu'il en soit, il faut désormais tenir compte du drone comme il faut tenir compte d'autres objets courants qui peuvent être détournés à des fins malveillantes. Cela n'est pas évident : en effet, comment par exemple empêcher une voiture-bélier ? On protège désormais l'accès aux grands rassemblements. Mais on ne pourra jamais faire face à toutes les occurrences, comme l'attentat de London Bridge. Il faut également tenir compte du risque d'importation - sur lequel nous avons également rédigé un rapport – des modes opératoires constatés sur les théâtres d'opérations. Dans la guerre des villes, à Mossoul et à Raqqa, Daech a notamment fait un usage fréquent des drones, à des fins de surveillance mais aussi d'attaque. C'est un risque sécuritaire à prendre en grande considération.

S'agissant des « bons » et des « méchants », nous sommes tous amis et ennemis dans tel ou tel domaine. Américains, Russes, Chinois, Britanniques, Français, Israéliens, mais aussi Iraniens et Nord-Coréens sont tous des acteurs cyber. Dans ce domaine, il faut s'attendre à une prolifération de la matière grise, à l'image de la prolifération nucléaire avec les réseaux Khan ; là est le risque. Parmi les « méchants », les terroristes s'intéressent au cyber, comme l'illustrent leur propagande et leurs actes de défiguration de sites, mais ils n'ont pas passé de cap technologique supérieur. Néanmoins, il est facile d'acheter les capacités nécessaires, surtout avec l'argent que génère le *dark web*, et de mercenariser des personnes. Dès lors, un État disposant de quelque richesse et résolu à s'en donner les moyens se mettra en quête de brillants ingénieurs informatiques et leur offrira une rémunération élevée ; ainsi, alors qu'il n'était pas d'emblée signalé comme tel, il se trouvera en mesure de mener une attaque.

**M. Stéphane Trompille.** Un rapport de spécialistes internationaux vient précisément de paraître dans différents journaux sur l'intelligence artificielle et la cybercriminalité. Vous avez parlé de manipulation politique – il y est fait référence dans ce rapport – ainsi que de drones tueurs – la science-fiction rattrapant en l'occurrence la réalité. Qu'en est-il de la prise de conscience en France de la manipulation de l'intelligence artificielle ?

**M. Jean-Jacques Ferrara.** Ma question, plus générale, pourra vous sembler naïve ou prématurée, voire les deux, Monsieur le secrétaire général. L'armée de l'air a attendu 1934 pour devenir autonome avec la création de son état-major. N'aurait-il pas fallu profiter de cette loi de programmation pour enclencher la mise en œuvre d'une véritable armée cyber autonome et interarmées pour faire face aux menaces et aux enjeux actuels, afin d'accélérer la montée en puissance de cette nouvelle arme en planifiant la formation, la transformation et le recrutement d'un personnel hautement qualifié ?

**M. Thomas Gassilloud.** La loi de programmation prévoit une montée en puissance du volet cyber, et c'est très bien, car nous pourrons ainsi renforcer notre présence sur le champ de bataille cyber. Cela étant, une présence massive sur le champ de bataille numérique ne suffit pas ; nos soldats doivent également disposer de capacités techniques à la hauteur des menaces, plus encore que dans le champ cinétique, car c'est la technologie qui, à l'avenir, fera la différence.

Dans le champ cyber, s'il est une technologie qui fera la différence, c'est l'informatique quantique, car elle changera totalement la donne en termes de puissance de calcul et produira des effets aussi importants que l'arrivée de la poudre sur le champ de bataille. Grâce au quantique, des opérations nécessitant en théorie des milliards d'années de calculs deviendront réalisables dans des délais raisonnables, ce qui aura pour conséquence d'annuler nos capacités de cryptographie et d'accélérer le développement de l'intelligence

artificielle. Face à un algorithme puissant, un millier de nos soldats, même équipés des meilleurs claviers, se trouveront en grande difficulté.

Je suis donc inquiet, Monsieur le secrétaire général, et je crois que c'est le rôle des parlementaires de l'être. En effet, je lis ceci à la page 181 du rapport *Chocs futurs*, du SGDSN : « Rien ne permet d'affirmer que le développement d'ordinateurs quantiques sera possible d'ici 2030. » Or, M. Becht et moi-même étions la semaine dernière aux États-Unis, où tous nos interlocuteurs nous ont annoncé l'apparition du quantique dans quelques années seulement et indiqué que des prototypes existent déjà. Pourtant, dans votre rapport de 187 pages, le mot « quantique » n'apparaît pas une seule fois, non plus d'ailleurs que les mots « puissance » et « supercalculateur ». Si je suis rassuré par la prise de conscience, je m'inquiète donc de nos moyens d'action car nous courrons de grands dangers si nous laissons à d'autres États ou au secteur privé le soin de développer des technologies qui assureront demain notre souveraineté. Vous avez à juste titre parlé de *Far West* numérique – une situation contraire à la raison d'être de l'État. Pouvez-vous donc nous rassurer sur le fait qu'au-delà des moyens humains consacrés au cyber, notre pays a bien pris en compte la nécessité de déployer une stratégie industrielle dans le domaine de l'informatique quantique ?

**M. Stéphane Demilly.** À partir de la page 65 de la revue stratégique de la cyberdéfense, Monsieur le secrétaire général, vous formulez des recommandations relatives à la protection des collectivités territoriales face à la cybercriminalité. Vous évoquez notamment le cas des régions, en raison de leurs compétences dans le domaine économique ; de manière générale, vous soulignez la masse d'informations que recueillent les collectivités et l'intérêt stratégique que revêt leur protection. Existe-t-il de ce point de vue un dialogue précis entre le SGDSN et les associations d'élus – régions, départements, communes – voire un dialogue direct avec certaines collectivités ? Je pense en particulier aux petites communes, dans lesquelles vous soulignez que l'absence de relais internes fait perdre son efficacité aux actions de sensibilisation qui sont menées.

**Mme Nicole Trisse.** Dans votre revue stratégique de la cyberdéfense, vous évoquez une réponse diplomatique conjointe de l'Union européenne face aux cyberattaques et un cadre européen de gestion des crises cyber, vous encouragez le développement de la coopération opérationnelle au sein de l'Union et vous vous dites favorables à une gouvernance collective et maîtrisée du cyberespace. Pouvez-vous nous en dire plus sur la mise en place de cette coopération et, surtout, sur ce qu'en pensent nos voisins européens ? Avez-vous eu l'occasion d'évoquer le sujet avec eux ?

**M. Patrice Verchère.** Ma question porte sur les ressources humaines. Avec l'apparition et le développement de la cybermenace, la loi de programmation place à juste titre la cybersécurité au rang de ses priorités et prévoit le recrutement, d'ici à 2025, de mille cybersoldats. Ne risquez-vous pas d'être confrontés à un problème de recrutement ? En effet, les entreprises sont très demandeuses – et l'ANSSI joue bien son rôle en les incitant à prendre des mesures. Comment garantir votre attractivité, alors que la grille indiciaire de la fonction publique ne risque guère de séduire des jeunes à qui des entreprises proposeront des rémunérations beaucoup plus élevées ? Comment réagirez-vous ?

**M. le président.** Hélas, ce n'est pas le seul métier concerné par ce problème…

**Mme Séverine Gipson.** Nos femmes et nos hommes engagés sont conscients des nouveaux enjeux et menaces et des nombreux défis à venir en matière de cyberdéfense. Cependant, cette dimension de la sécurité ne concerne pas seulement nos militaires, mais aussi les entreprises et les administrations publiques. Quels outils et mesures estimez-vous nécessaires afin de sensibiliser les uns et les autres à ces nouvelles menaces ?

**M. Louis Gautier.** Notre REVUE, Monsieur Trompille, aborde la question de l'intelligence artificielle et des automates, mais il renvoie aussi au rapport Villani ; nous ne pouvions pas tout traiter, tant cet horizon est immense. Nous décrivons un scénario d'attaque bien connu, partant de caméras de vidéosurveillance. En clair, le constat est fait. En revanche, il sera très difficile pour nos sociétés de déterminer comment marier la sécurité par domaine et par métier, d'une part, et la cybersécurité, d'autre part. En ce qui me concerne, je pense que c'est la sécurité par domaine et par métier qui doit l'emporter en matière de direction et de conception. Dès lors, les métiers concernés doivent acculturer la problématique cyber.

Je m'explique : lorsque circuleront des voitures autonomes et interconnectées, la priorité à droite demeurera. Dans le domaine de la santé où se multiplient les sondes et autres *pacemakers*, régulés à distance, c'est évidemment la connaissance biologique de l'organisme qui dirige et qui permet de décrire le moment de dangerosité, voire de rupture, contre lequel il faut à tout prix se protéger. C'est la principale difficulté : on a l'impression que le cyber est projeté de l'extérieur par des spécialistes de la question, qui ajoutent une couche supplémentaire de sécurité à la problématique numérique – c'est ainsi que l'on pensait autrefois. Aujourd'hui, il faut, dès leur conception, penser l'intégration de la sécurité dans le développement de ces multiples artefacts connectés. C'est dès le départ, dès l'étape de leur invention que la sécurité doit être prise en compte dans l'architecture des systèmes. Or, ces métiers, qui reposent de hautes compétences scientifiques et technologiques, sont très en retard dans la prise en compte de la sécurité : le numérique ne représente souvent pour eux qu'une fonctionnalité parmi d'autres, qui les aide dans leur travail. La fonctionnalité, la sûreté priment. La sécurité qui implique la prise en compte des risques extérieurs à et liés à son environnement est une dimension encore assez mal prise en compte.

De ce fait, généraliser l'intelligence artificielle sans avoir complètement saisi les logiques de sécurité à l'œuvre dans la société nécessite une profonde évolution du dialogue avec les utilisateurs, qui comptent sur des agences et autres prestataires pour sécuriser leur environnement cyber, et à qui nous devrons dire qu'il nous faut travailler d'emblée avec eux et qu'il leur faut pour ce faire intégrer la problématique cyber, car elle est au cœur de l'automate, de la puce, de la sonde d'insuline, mais aussi de la transmission de l'information, des bases de données, etc.

J'en viens à la question de l'autonomie de l'armée cyber, Monsieur Ferrara. Il faut en effet développer les moyens militaires, mais j'ai essayé de montrer que si toutes les missions doivent être coordonnées, elles ne peuvent pas être superposées ni intégrées. En particulier, le modèle français et européen diffère du modèle américain où la *National Security Administration* (NSA) fait office de grande agence technique pour l'ensemble des services de renseignement, à quoi s'ajoutent d'innombrables doublons. En France, tout ne sera pas fait par le ministère des Armées et, à l'évidence, tout ne doit pas être fait par lui. Qu'il s'agisse des entreprises ou de l'intelligence artificielle, ce sont des problématiques qui ne peuvent pas être intégrées au sein d'un seul ministère selon l'idée quelque peu fantasmatique d'une armée cyber qui ferait tout ; ce n'est pas la bonne approche. Il n'empêche qu'une armée cyber est

nécessaire pour sécuriser nos dispositifs militaires et pour trouver les failles de nos adversaires.

Le rapport que nous avons produit au printemps dernier, *Chocs futurs*, aborde la question de l'ordinateur quantique, Monsieur Gassilloud, mais avec précaution : nous y évoquons l'exemple canadien dans ce domaine et d'autre cas « disruptifs » où il est impossible de prévoir s'ils se réaliseront à court terme. Il existe en revanche des changements certains mais progressifs : on sait par exemple que le processus de robotisation du champ de bataille est enclenché, et il ne fait aucun doute qu'il faut déjà se préoccuper de cette évolution en cours. Le quantique, en revanche, progresse à coup de sauts technologiques dont on ne peut pas prouver qu'ils se produiront à tel ou tel moment ; c'est pourquoi nous estimons qu'ils pourront avoir lieu d'ici à 2030. L'exemple canadien existe certes, mais nous restons prudents et ne sommes pas certains d'avoir fait ce saut d'ici à une quinzaine d'années. Cependant, ce saut représentera à l'évidence une révolution, comme vous l'avez dit. Le rapport ajoute d'ailleurs que des révolutions ont été faites dans d'autres domaines sans pour autant que l'on y prête une grande attention : les ciseaux génétiques CRISPR-Cas9, une biologie de garage qui permet à n'importe qui de faire du génie génétique, susciteront l'émergence de *hackers* biologiques comme il existe aujourd'hui des *hackers* informatiques. De même, l'imprimante 3D permettrait d'obtenir des résultats formidables, mais notre pays est très en retard par rapport à l'Allemagne, par exemple. Autrement dit, des révolutions technologiques existent et vont produire des effets sociétaux, économiques et stratégiques majeurs, et l'on n'y prête pas ou peu attention. Quoi qu'il en soit, vous avez raison, Monsieur Gassilloud : nous nous dirigeons vers la révolution quantique, mais j'ignore quand exactement.

**M. Thomas Gassilloud.** Pas avant 2030, nous dites-vous, mais ce n'est pas ce que l'on entend ailleurs…

**M. Olivier Becht.** IBM nous a dit : dans cinq ans !

**M. Louis Gautier.** Entre 2023 et 2030, je veux bien débattre de la date ; nous prônons la prudence, mais cette révolution devrait en effet se produire dans les quinze ans qui viennent – ce qui, à perspective humaine, n'est rien.

Nous avons abordé dans le rapport la question des collectivités locales, Monsieur Demilly, sans entrer dans plus de détails car il faut travailler davantage en impliquant avant tout les collectivités elles-mêmes. Deux pistes s'offrent à nous : la première a consisté, depuis 2015, à créer des délégations régionales de l'ANSSI, qui sont autant de têtes de pont fournissant des contacts aux associations d'élus et aux collectivités locales. La deuxième piste est celle de la plateforme Acyma, que nous avons mise en place à l'automne dernier : elle s'adresse avant tout aux PME mais peut aussi concerner les collectivités locales, car elle vise entre autres à diffuser les bonnes pratiques, et à mettre en contact des victimes et des prestataires de services de sécurité que l'ANSSI référence, même si elle ne les agrée pas. Cette dernière action se fait à l'échelle locale : que vous soyez à Roubaix, à Cassis, à Aix, à Nîmes ou ailleurs, vous aurez la possibilité de trouver, selon votre demande, une liste des prestataires référencés et notés par les usagers – une sorte de « booking.com » de la sécurité informatique. Les collectivités locales peuvent utiliser cette plateforme même si, à l'origine, elle a plutôt été conçue pour lutter contre la cybercriminalité dans les PME.

En Europe, Madame Trisse, Guillaume Poupard et l'ANSSI comme moi-même entretenons des contacts extrêmement fréquents – au moins une fois par mois en ce qui me concerne – avec nos principaux partenaires, l'Allemagne et le Royaume-Uni notamment. Je rappelle que c'est un Français issu de l'ANSSI qui préside le conseil d'administration et le conseil exécutif de l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information, à travers laquelle nous nous employons à développer un champ de convergence réglementaire. Toutefois, les niveaux techniques et technologiques au sein de l'Union sont très hétérogènes : nos principaux partenaires, que j'ai cités, sont au même niveau que nous ; pour le reste, notre action consiste surtout à apporter notre aide et à favoriser les bonnes pratiques. Il va de soi que l'Union européenne doit se saisir de cette question, mais nous ne souhaitons pas l'européanisation de notre cyberprotection dans la mesure où nous avons un train d'avance – et c'est heureux –, en ce qui concerne les attaques les plus graves et les plus virulentes notamment. Cela étant, la revue stratégique préconise des coopérations : si un État européen était attaqué, l'ANSSI mettrait naturellement ses savoir-faire à sa disposition pour l'aider à résoudre le problème.

S'agissant des entreprises, Madame Gipson, j'ai déjà évoqué la plateforme Acyma. Pour élever le niveau, les normes professionnelles sont un vecteur pertinent. Prenons pour exemple l'attaque perpétrée contre Saint-Gobain, qui aurait provoqué, selon les déclarations publiques de l'entreprise, une perte de chiffre d'affaires de l'ordre de 80 millions d'euros sur son résultat d'exploitation et de 250 millions d'euros sur ses ventes. Une telle somme, que je ne commenterai pas, pèse sur un bilan et sur la cotation en bourse ! L'ANSSI ne déclare d'ailleurs jamais le nom des entreprises auxquelles elle vient en aide, afin d'éviter de les fragiliser face à la concurrence. Les entreprises elles-mêmes, en revanche, sont parfois contraintes de communiquer ces données car leurs actionnaires vont constater une perte dans le bilan. En somme, toutes les normes professionnelles qu'il faudrait mettre en œuvre, qu'elles soient comptables, assurancielles – sur le risque cyber – ou qu'elles concernent la notation du risque cyber, notamment pour les sociétés cotées en bourse, contribueront grandement à la prise de conscience et la culture de la cybersécurité dans les entreprises.

Vous avez tout à fait raison, Monsieur Verchère : le recrutement est un point de butée pour nous tous. Nos écoles sont plutôt performantes, et nos ingénieurs et techniciens sont d'un niveau satisfaisant ; de ce fait, justement, on nous les « pique », si j'ose dire. La première concurrence se trouve donc au sein de l'État. La deuxième concurrence oppose l'État et les entreprises ; enfin, la troisième concurrence est internationale, les Américains notamment offrant des rémunérations très élevées. Nous sommes conscients qu'il est indispensable d'augmenter l'offre de formation. L'ANSSI, dont les effectifs ont augmenté de 50 personnes par an dans les années passées et de 25 aujourd'hui, parvient à gérer son recrutement parce qu'elle est attractive et s'apparente aussi pour les jeunes agents à une phase de formation et d'expérience professionnelle fortement valorisable dans la suite de leur carrière ; les mouvements de personnel sont inévitables, mais ils permettent aussi d'essaimer. Il est vrai, cependant, que nous peinons à réguler les recrutements, entre les employés que nous acceptons de laisser partir – à condition que ce soit après deux ou trois ans, et non pas seulement à l'issue de l'année initiale de formation – et ceux que nous souhaitons garder pour sédimenter de l'expérience, de la compétence et de l'encadrement. C'est un sujet majeur et difficile : en termes d'offre de formation, nous ne sommes pas à la hauteur des enjeux qui se présenteront au cours des dix prochaines années.

**M. Jacques Marilossian.** Le projet de LPM prévoit un renforcement notable de la sécurité, notamment en matière d'effectifs. Parallèlement, il nous est également annoncé des investissements d'un montant de 11 milliards d'euros dans les infrastructures de défense pour la période 2019-2025. Ma question est donc simple : pour réaliser notre ambition en matière de cyberdéfense, quelle est la part de ce montant de 11 milliards qui sera consacrée aux infrastructures dédiées à la cyberdéfense ? Plus directement, avez-vous une idée de la répartition de ces crédits entre les bâtiments et travaux publics, le matériel, les logiciels ? Des plans de reprise d'activité (PRA) et des plans de continuité des opérations (PCO) sont-ils prévus ? Quelles sont vos priorités à cet égard ?

**Mme Françoise Dumas.** Les États membres de l'Union européenne se sont accordés pour apporter une réponse diplomatique conjointe aux crises cyber en mettant en œuvre des mécanismes de coopération internationale en matière de prévention et de sanction. Comment la coopération entre l'Union européenne et l'OTAN va-t-elle selon vous se développer dans ce domaine, étant donné que certains membres de l'OTAN ne sont pas membres de l'Union, ce qui confère une place particulière à la France, au regard non seulement de ses obligations internationales mais aussi de sa place plus que singulière au sein de l'OTAN ?

**M. Loïc Kervran.** Ma question porte sur l'article 19 du projet de loi et le cadre de contrôle du recueil et de l'analyse des métadonnées par l'ANSSI. Quelle analyse faites-vous des différences avec le dispositif prévu à l'article L. 851-3 du code de la sécurité intérieure, vulgairement appelé « boîte noire » ? J'entends naturellement que les utilisateurs et que l'objet même diffèrent, puisque l'article L. 851-3 ne vise que les actes de terrorisme. Cependant, les capacités de recueil prévues par ces deux dispositifs sont-elles différentes ? Est-il envisagé un processus de désanonymisation comme c'est le cas pour les objectifs de terrorisme ? Une intervention de la commission nationale de contrôle des techniques de renseignement (CNCTR) est-elle prévue ?

**Mme Sabine Thillaye.** Nous avons abondamment souligné la souveraineté numérique, en France comme dans l'Union européenne. Si l'internet n'a pas de frontières, il est tout de même dominé par des entreprises extra-européennes, en particulier américaines. Sur un sujet dépassant quelque peu le cadre de la défense, j'ai récemment été alertée par des *hackers* – de « bons » *hackers* – sur l'attribution par la Commission européenne, en novembre, du programme d'analyse de vulnérabilité du lecteur multimédia VLC à l'entreprise américaine HackerOne. Ce programme dit de *bug bounty*, c'est-à-dire d'externalisation de la détection des vulnérabilités en matière de cybersécurité, s'inscrit dans le cadre du projet européen FOSSA d'audit des logiciels libres et *open source* utilisés par la Commission.

Il me semble que le choix d'une société américaine pour détecter les failles existant dans nos entreprises a de quoi surprendre eu égard aux enjeux de souveraineté numérique. Jugez-vous opportun d'introduire une clause de préférence européenne dans les appels d'offres et marchés publics dédiés ?

**M. Thibault Bazin.** Vous avez évoqué les nécessaires actions en justice, mais il y a peu de plaintes, ce qui limite notre connaissance de l'ampleur des attaques. Quels seront les moyens supplémentaires alloués à la police judiciaire et à la justice pour lutter contre la cyberdélinquance ?

Concernant la protection des données, si l'on est cyberconscient, on ne peut pas faire confiance aux pays amis, il faut même s'en méfier. Avec 2 000 entreprises françaises suivies secret-défense ou équivalent, quelles modifications sont à envisager ? Ne faut-il pas poser des limites à la coopération européenne pour protéger les données, et maintenir ces entreprises sous l'empire du droit français ? Cette question revient régulièrement au sein de la mission d'information sur la cyberdéfense, conduite par mes talentueux collègues.

**M. Christophe Lejeune.** La Corée du Nord a pu se doter de l'arme nucléaire pour deux raisons : un apport de technologie, et la capacité à générer des flux financiers entrants et sortants malgré des embargos et sanctions économiques et financières.

Ce matin, vous avez évoqué le *dark web* et la cryptomonnaie. Pensez-vous qu'une des raisons du succès des monnaies virtuelles soit l'attrait des organisations criminelles et des pays sous régime de sanctions – que vous combattez – pour la discrétion qu'elle leur offre ? Dans l'affirmative, quelles actions de cyberdéfense menez-vous, et pensez-vous qu'une législation supranationale encadrant la cryptomonnaie devrait être envisagée ?

**M. Philippe Michel-Kleisbauer.** Avant de poser ma question, je me permets de dire que vous nous avez offert l'une des auditions les plus passionnantes que nous ayons eues, et je pense que ce sentiment est partagé par mes collègues.

Ma question est une forme de conclusion au débat : ne devons-nous pas circonscrire la coopération en cyberdéfense à un nombre restreint d'États ? Et parallèlement à ce que vous disiez de la doctrine de dissuasion, devons-nous dénier l'accès à certaines techniques et technologies aux autres ?

**M. Louis Gautier.** L'effort consacré au cyber s'élève à peu près à 1,6 milliard d'euros sur toute la période de programmation. C'est la ministre des Armées qui pourra vous donner la ventilation entre les infrastructures, les dépenses d'équipement ou les investissements en recherche et formation.

S'agissant de l'Union européenne et de l'OTAN, la question soulevée précédemment m'a permis d'apporter des réponses. L'OTAN est un mécanisme de sécurité collective, l'Union européenne, c'est autre chose. Cela a aussi été évoqué par d'autres intervenants, notamment s'agissant de l'externalisation de la détection, l'Union européenne a un champ de protection numérique, de souveraineté européenne, beaucoup plus vaste. Dans nos quatre chaînes opérationnelles, l'OTAN correspond à la mobilisation de l'action militaire.

Mais, pour répondre à la question posée sur les juges, la police et la gendarmerie, nous avons un parquet financier, un parquet antiterroriste, nous pourrions avoir des juges cyber. Et les enquêtes ne peuvent pas être menées uniquement en France ; il faudrait un parquet européen ; c'est à ce niveau d'agrégation que l'on pourrait faire quelque chose, y compris pour les sanctions. Les États ne sont pas seuls à se livrer à la captation de données. Dans le champ économique, c'est aussi le fait d'entreprises qui veulent racheter un concurrent, avoir accès à un brevet ou à une information privilégiée éventuellement utile dans le cadre d'une négociation commerciale, d'une transaction ou d'une procédure judiciaire. Dans ce domaine, qui relève plus de la sécurité numérique que du champ économique, ce n'est pas l'OTAN qui est pertinente.

Comment se fait la différenciation ? L'OTAN a en charge la sécurité collective, pour répondre à des situations comme celle de l'Estonie. La question est celle de notre réaction, et notamment des contre-mesures éventuelles, voire des intrusions et des actions agressives dans le champ cyber. Répliquerons-nous de cette manière, voire même au-delà ?

Monsieur Kervran, votre question va me permettre de décrire une voie alternative, qui n'a pas été choisie. Rappelez-vous l'article L. 851-3 du code de la sécurité intérieure, qui concerne le terrorisme. Cet article très particulier a été voté dans un contexte précis, d'urgence, pour lutter contre le terrorisme. Et rappelez-vous la manière dont le Conseil constitutionnel a approuvé cette exception en raison de la nature de la menace terroriste et en posant certains considérants constitutionnels préalables impliquant de pouvoir circonscrire et contrôler l'exploitation des données collectées dans le cadre de la lutte contre le terrorisme. Or la menace cyber est, de manière globale, assez peu discriminée. Elle va de la compromission de données sur un téléphone portable aux actions de longue main que j'ai évoquées plus tôt, et qui impliquent toute une stratégie sur plusieurs mois pour s'infiltrer et capter les données.

On ne peut pas imaginer la fabrication d'un algorithme pertinent permettant de procéder à un tri dans des volumes massifs de métadonnées stockées jusqu'à leur exploitation.

En outre, la loi relative au renseignement concerne un travail des services, impliquant une temporalité séquencée : une enquête de terrain ; la demande d'interception de sécurité ; la consultation de la CNCTR ; l'autorisation du Premier ministre ; l'interception et l'analyse des données. S'agissant de la lutte contre le terrorisme, si l'on sait qu'une personne donnée est partie en Syrie, il est possible de collecter des informations auprès de sa parentèle, d'analyser des communications. C'est un travail qui peut prendre le temps nécessaire pour que l'enquête permette de purger toutes les dangerosités, par exemple à partir d'un numéro trouvé dans le téléphone d'un terroriste après l'attentat du Bataclan.

Nous ne sommes pas du tout dans cette logique, ni dans cette temporalité s'agissant du risque cybernétique. Nous devons faire une détection immédiate, de façon à intervenir en temps réel, pour empêcher l'attaque. Agir au plus près et au plus vite. D'où cet article 19 de la LPM qui met en place un système de tamisage des flux et qui ne porte que sur la détection et l'analyse de données techniques de communication.

Dans le domaine du renseignement et de la lutte contre le terrorisme, c'est un travail d'enquête dont le but est de tracer une filière pour la démanteler ou de rechercher l'origine d'une action hostile. Quelque chose de troublant a déjà été identifié, Des indices ont été relevés et les services cherchent à en découvrir l'origine.

D'une certaine manière, c'est le travail que réalise *ex post* le procureur spécial Robert Mueller dans son enquête sur les ingérences dans l'élection américaine de novembre 2016. Il en est au stade où il analyse dans son rapport la campagne de déstabilisation et de « fake news ». Il progresse mais n'est pas encore parvenu à caractériser les attaques contre le parti démocrate.

En matière de cyberdéfense, nous ne sommes pas du tout dans cette temporalité-là : nous devons détecter l'attaque pour la prévenir ou la contrer le plus vite possible, nous devons repérer le *malware* ou le virus, de façon à protéger la victime et à empêcher que cette

attaque vienne contaminer les systèmes d'information de l'État ou des opérateurs d'importance vitale.

Ces deux raisons, à la fois opératoires et logiques, s'ajoutent au fait que nous voulons rester cohérents avec notre modèle, qui prévoit que la détection et la remédiation SONT du ressort de l'ANSSI, et non pas des services de renseignement. L'ANSSI est en effet une agence interministérielle qui ne s'intéresse pas aux contenus, et n'aurait d'ailleurs pas les moyens de les exploiter : il n'y a pas d'analystes à l'ANSSI qui s'intéressent à la nature des messages. Ce sont des métadonnées qui sont conservées, puis détruites, quand des virus ont été détectés sur des systèmes d'importance vitale. Prévoir un contrôle de l'ANSSI par la CNCTR aurait introduit de la confusion : cela serait revenu à dire que la même organisation était censée contrôler à la fois les interceptions de sécurité des services de renseignement et des détections qui, justement, ne sont pas des interceptions de sécurité dans la mesure où elles ne s'intéressent pas au contenu. C'est pourquoi nous avons préféré en charger l'ARCEP : d'abord parce dans le système collaboratif mis en place, il est de la compétence de l'ARCEP de contrôler ce que font les opérateurs conformément au code des communications électroniques ; ensuite parce selon les dispositions de l'article 19. Il lui reviendra de vérifier que l'action de l'ANSSI ne déborde du cadre précisé par la loi.

Ce système va dans le sens de la consolidation de notre modèle, de la claire distinction des missions entre celles de l'ANSSI et celles des services spécialisés de renseignement. Le portage est très différent de celui prévu par la loi de 2015 sur le renseignement ; le contrôle doit l'être aussi. Je rappelle que ce qui a été fait sur l'article L. 851-3 du code de la sécurité intérieure a été fait dans un cadre très utile pour les services de renseignement, mais qui n'est pas de même nature.

Il est vrai que nous allons devoir renforcer les moyens des services de renseignement, notamment pour procéder aux attributions. Il y a de l'enquête humaine, mais il y a aussi une partie scientifique, qui doit aller au-delà de ce que fait l'ANSSI. Cette dernière n'est d'ailleurs pas toujours directement impliquée : elle n'intervient que s'il s'agit d'opérateurs d'importance vitale ou de services de l'État. Il se peut qu'un service de renseignement, pour une raison de sécurité économique ou de cybercriminalité, ait à travailler sur cette matière, notamment pour localiser le commanditaire de l'action. Ce champ du renseignement doit être développé, dans le cadre de la loi sur le renseignement, qui fixe par ailleurs les objets de chacun de ces services.

Sur la cyberdéfense, je pense avoir globalement répondu. Il est nécessaire de réévaluer les politiques de cyberdéfense, en conservant l'idée que nous y parviendrons bien si nous discriminons ce que chacun doit faire opérationnellement. La protection est une fonction, le renseignement ou l'action militaire sont d'autres fonctions.

S'agissant de la cyberdélinquance et des limites de la coopération européenne, il est nécessaire de renforcer l'Europe à ce niveau. Il faut au moins un réseau de juges compétents en la matière.

Sur la Corée du Nord, je suis d'accord ; si nous pouvions obtenir une régulation ou une législation internationale permettant de dissuader l'usage de certaines cryptomonnaies, ce serait une bonne chose. Lors du séminaire de lancement de la Revue organisée à l'École militaire, en septembre dernier, nous avons appris d'un intervenant qu'au Japon, il était

possible jusqu'à il y a peu de payer ses impôts en *bitcoins*, ce qui revient à légaliser le *bitcoin*. Il n'y a donc pas de consensus entre pays pour décider si le *bitcoin* est toléré, légal illégal. Il faut à cet égard faire la différence entre les différents types de cryptomonnaies.

**M. le président.** Je vous remercie, Monsieur le secrétaire général, vous avez été très complet.

*La séance est levée à douze heures cinquante.*

*

*  *

**Membres présents ou excusés**

*Présents.* - M. Louis Aliot, M. François André, M. Pieyre-Alexandre Anglade, M. Jean-Philippe Ardouin, M. Thibault Bazin, M. Olivier Becht, M. Christophe Blanchet, Mme Aude Bono-Vandorme, M. Jean-Jacques Bridey, M. Philippe Chalumeau, M. Jean-Pierre Cubertafon, M. Stéphane Demilly, Mme Marianne Dubois, Mme Françoise Dumas, M. Olivier Faure, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Laurent Furst, M. Claude de Ganay, M. Thomas Gassilloud, Mme Séverine Gipson, M. Guillaume Gouffier-Cha, M. Fabien Gouttefarde, Mme Émilie Guerel, M. Jean-Michel Jacques, M. Loïc Kervran, M. Bastien Lachaud, M. Fabien Lainé, Mme Frédérique Lardet, M. Didier Le Gac, M. Christophe Lejeune, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, M. Joaquim Pueyo, M. Gwendal Rouillard, M. Antoine Savignat, Mme Sabine Thillaye, Mme Laurence Trastour-Isnart, Mme Nicole Trisse, M. Stéphane Trompille, M. Patrice Verchère, M. Charles de la Verpillière

*Excusés.* - M. Damien Abad, M. Bruno Nestor Azerot, M. Florian Bachelier, Mme Carole Bureau-Bonnard, M. Luc Carvounas, M. André Chassaigne, M. M'jid El Guerrab, M. Richard Ferrand, M. Marc Fesneau, M. Christian Jacob, Mme Anissa Khedher, M. Jean-Christophe Lagarde, M. Jean-Charles Larsonneur, M. Franck Marlin, Mme Natalia Pouzyreff, M. François de Rugy, M. Thierry Solère, Mme Alexandra Valetta Ardisson