ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information sur l'actualisation de la LPM 2019-2025

Mardi
8 juin 2021
Séance de 17 heures 30

Compte rendu n° 62

SESSION ORDINAIRE DE **2020-2021**

Présidence de Mme Patricia Mirallès, *vice-présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures trente.

Mme Patricia Mirallès, présidente. Monsieur le directeur général, notre présidente, Mme Françoise Dumas, empêchée car elle se trouve à l'étranger dans le cadre de la mission qu'elle préside sur la stabilité du Moyen-Orient dans la perspective de « l'après Chammal », m'a demandé de vous transmettre ses excuses. Nous nous réjouissons de vous accueillir dans le cadre de notre cycle sur l'actualisation de la loi de programmation militaire (LPM). Lors de votre dernière audition devant notre commission, il y a un peu plus d'un an, vous nous avez dit que des attaquants de toute nature tentaient de tirer parti de la numérisation croissante de notre société. Vous avez aussi indiqué que la pandémie augmentait l'exposition de nos concitoyens à la menace cybernétique, le recours massif et rapide au télétravail renforçant les risques courus par les systèmes d'information des administrations publiques, ce compris les établissements de santé et les collectivités territoriales, et par nos entreprises. De plus, l'actualisation stratégique 2021 a souligné que le cyberespace est devenu, comme l'espace physique, un champ de rivalités stratégiques, voire de conflictualité.

Créé en 2009 et rattachée au secrétaire général de la défense et de la sécurité nationale, le SGDSN, l'Agence nationale de la sécurité des systèmes d'information, l'ANSSI, que vous dirigez, a développé des dispositifs de cybersécurité robustes et performants. Elle a bénéficié de moyens croissants, son effectif passant de 100 personnes lors de sa création à 600 aujourd'hui. Les LPM successives ont renforcé les missions et les pouvoirs de l'Agence. L'effort est marqué dans la LPM 2019-2025, qui contient plusieurs dispositions relatives au renforcement des capacités de détection, de caractérisation et de prévention des attaques informatiques. Dans la même ligne, la ministre, lors de son audition par notre commission le 4 mai dernier, a fait de l'axe « Mieux détecter et contrer » le premier axe prioritaire des futurs ajustements de la LPM, avec l'objectif de développer nos capacités défensives en matière de cyberdéfense et de numérique.

Vous nous ferez part de l'actualité de vos missions, notamment celle qui vous est dévolue par l'article 34 de la dernière LPM relatif à la cyberdéfense, des moyens dont vous disposez pour les remplir et nous direz s'ils sont toujours suffisants pour faire face à des attaques qui se multiplient. Vous nous signalerez les points de vigilance éventuels. La ministre ayant évoqué devant nous les espoirs qu'elle place dans le programme d'intelligence artificielle Artémis et le data center de Bruz, vous nous expliquerez ce que vous en attendez.

Lors de votre précédente audition, vous aviez indiqué que deux cercles se dessinaient, le premier englobant les nations capables d'assurer leur souveraineté numérique, petit club au sein duquel vous rassembliez les États-Unis, la Chine, la Russie et Israël, et un second cercle de pays se plaçant sous la protection du premier. Pensez-vous que la France ait les capacités budgétaire, technologique et industrielle de se compter au nombre des grands ? Comment éviter tout risque de déclassement ?

M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information. Trois types de menaces nous obligent à adapter en permanence nos dispositifs de défense, de détection et de réaction. La France veut être une puissance en matière de cybersécurité, mais étant donné ceux contre qui nous luttons, la disproportion des moyens rend essentiel le bon emploi de nos ressources. À ce titre, je rappelle en permanence à

mes équipes que l'inefficacité n'est pas concevable. Cette approche vaut en interne comme avec tous nos partenaires publics et privés au niveau national, et à l'échelle européenne.

Le premier phénomène, visible et médiatisé, est le développement de la grande criminalité. Celle-ci utilise un procédé pour l'instant difficile à parer consistant à s'en prendre à des cibles très variées à des fins d'extorsion. Les criminels pénètrent les réseaux, volent les données et les chiffrent pour les rendre inaccessibles à leurs victimes. Les cyberattaquants demandent ensuite le versement de rançons, de plusieurs millions d'euros, en bitcoins ou en d'autres cryptomonnaies, beaucoup plus difficiles à tracer que les devises classiques. Tous les moyens de chantage sont alors bons pour obtenir ces rançons. « Ou vous payez », disent-ils, « ou vous ne récupérez pas vos données, et nous allons même en publier certaines sur internet ». Ce schéma de base a quelques variantes, ces criminels ayant une inventivité remarquable.

Les entreprises ainsi attaquées, devenues, comme l'ensemble des secteurs de la société, dépendantes du numérique, sont foudroyées. L'indisponibilité des données numériques entraîne des conséquences dramatiques et des pertes considérables. Que les victimes payent la rançon ou qu'ils s'y refusent, l'attaque leur coûte très cher. Il y a quelques mois, un grand industriel français a perdu ses réseaux en quelques minutes. Cela a conduit à une perte quotidienne de 10 millions d'euros, à laquelle s'ajoutent la perte de confiance des partenaires et clients et le stress enduré à l'idée de ne pas réussir à redémarrer. Les exemples de ce type sont multiples chez les grands acteurs économiques avec lesquels nous sommes en contact direct. Mais les attaques visent aussi des PME et des ETI, dont certaines ont malheureusement dû déposer leur bilan pour avoir perdu leurs données et ne pas être parvenues à les récupérer quand bien même elles auraient payé la rançon. Cette activité criminelle a donc un impact économique réel.

Mais les conséquences vont au-delà, puisque certains s'en prennent aussi à des hôpitaux, même au cours d'une crise sanitaire. Les attaques se sont enchaînées depuis que, fin 2019, le CHU de Rouen a été le premier touché. Je vais vous sembler cynique, mais cet épisode fut aussi une expérience intéressante, parce que nous alertions depuis un certain temps les hôpitaux sur la fragilité de leur système d'information et sur les risques qu'ils courraient s'ils perdaient leurs données. La réponse qui nous était faite peut se résumer à : « Oui, peut-être, mais il ne nous arrivera rien car nous ne sommes pas des cibles ». Or, les criminels attaquent les hôpitaux car ayant commencé par s'en prendre à de grandes cliniques américaines qui ont payé de très grosses rançons, ils ont poursuivi sur leur lancée, ignorant peut-être qu'un CHU français ne payera pas une rançon de plusieurs millions d'euros – mais le mal est fait et les hôpitaux deviennent des cibles.

L'attaque visant le CHU de Rouen a montré l'ampleur des conséquences de tels agissements : absence des dossiers administratifs, disparition des dossiers des patients, de l'imagerie, des analyses biomédicales… bref, plus rien pour accueillir des patients et les soigner. De plus, nous assurait-on lorsque nous faisions part de nos inquiétudes, n'ayez crainte, si jamais nous étions attaqués, les médecins savent encore soigner. Mais la réalité est autre : certes, dans un hôpital, on sait heureusement encore soigner les gens mais le nombre de personnes soignées a chuté drastiquement. Aussi, en termes de qualité des soins, les médecins eux-mêmes nous ont confié que certaines procédures sont désormais impossibles sans outils numériques et reconnaissent que devoir s'envoyer les constantes biologiques des patients sur des portables personnels est source d'erreurs. En pratique, le CHU de Rouen n'a

pu traiter que les urgences vitales pendant plusieurs jours. Après ce coup de semonce, malheureusement, les attaques se sont répétées. Au début de l'année 2020 en ont été victimes coup sur coup les hôpitaux de Dax, Villefranche-sur-Saône, Oloron Sainte-Marie et Saint-Gaudens. Il leur a fallu des semaines pour redémarrer, des mois pour revenir à une situation normale – et certains n'y sont toujours pas parvenus.

Je mentionnerai aussi l'attaque qui a marqué les esprits aux États-Unis il y a quelques semaines. Elle a visé Colonial Pipeline, l'opérateur du principal oléoduc de la côte Est, par lequel circule la moitié du pétrole raffiné de cet immense territoire. Tout a été arrêté ; vous imaginez sans mal les files de voitures et la pénurie qui s'installe faute de ravitaillement – et si l'opérateur ne ravitaillait plus, c'est qu'il était incapable de facturer. Outre que les cyberattaques peuvent viser n'importe quel secteur, cela nous montre que les vulnérabilités sont multiples et que les conséquences parfois inattendues. Autre enseignement majeur : Colonial Pipeline, qui a payé une rançon de 5 millions de dollars, n'a réussi à récupérer que 5 % de ses données. C'est dire que céder au chantage n'a pas d'effet magique.

Les collectivités locales sont d'autres victimes de cyberattaques qui ont un très fort impact sur la vie quotidienne de nos concitoyens. La principale attaque que nous avons dû gérer a visé l'agglomération d'Aix- Marseille, deux jours avant les élections municipales, probablement un simple concours de circonstances. Jusqu'au dernier moment, les fichiers n'étant plus accessibles, la ville a craint de ne pouvoir éditer les listes d'émargement. Beaucoup d'autres dysfonctionnements ont ensuite été observés, l'organisation des transports en commun a été affectée, comme la facturation de la distribution d'eau. Le plan des concessions n'étant plus accessible, les cimetières de Marseille ont été bloqués pendant une dizaine de jours, en pleine pandémie. Enfin, les chiffres liés à la pandémie n'ont pas pu être remontés. Cet épisode a rappelé que toutes les collectivités locales sont les cibles potentielles de cyberattaques dont l'impact est souvent bien plus important que pourrait le laisser croire une analyse trop rapide. Dans ce cas, la rançon demandée n'a pas été payée. Le cas des collectivités locales nous inquiète parce que leur niveau de sécurité informatique, globalement très insuffisant, les rend vulnérables à l'explosion exponentielle de la cybercriminalité. L'ANSSI a traité une cinquantaine d'attaques cybercriminelles en 2019, 200 en 2020 ; en ce moment, nous traitons en permanence un flux de ces cyberattaques.

La deuxième menace, c'est l'espionnage, phénomène le plus inquiétant mais qui n'est pas, ou peu, médiatisé, et mal compris quand il l'est. Les victimes n'ont pas envie d'en parler, les attaquants sont forts et discrets, et nous ne sommes pas là pour pointer du doigt les victimes mais pour les aider. Cependant, que tout reste secret conduit à mésestimer la question. Or, deux très grosses opérations mondiales ont été conduites depuis le début de l'année 2020. Le mode opératoire de la première est très intéressant : l'attaquant a piégé un logiciel majoritairement utilisé par les grandes entreprises et les grandes administrations des États-Unis, et par d'autres ailleurs. Le virus malveillant a été introduit dans une mise à jour d'un logiciel de la société SolarWinds légitimement utilisé par les victimes. Cette mise à jour a été téléchargée par 18 000 acteurs de premier plan à travers le monde, dont un millier en France.

Ce type de piratage est imparable, puisque la mise à jour régulière des logiciels est l'un des fondements de la sécurité informatique. Dans le cas qui nous occupe, l'attaquant, dépassé par le nombre de ses victimes potentielles, plus de 18 000, s'est concentré sur les grandes agences fédérales américaines, notamment dans le domaine de l'énergie et de la

défense. Il s’est également intéressé aux grands acteurs numériques que sont Cisco et Microsoft, qui ont été piégés bien qu’étant parmi les meilleurs au monde en termes de sécurité. Les Américains ont été particulièrement par cette cyberattaque, qui a aussi touché six institutions européennes. Nous avons dénombré, je vous l’ai dit, un millier de victimes potentielles en France, dont certaines avec des missions critiques, mais l’attaquant s’étant concentré sur des cibles américaines, aucune des failles présente chez des acteurs français n’a été exploitée. Les États-Unis ont désigné le SVR, service des renseignements extérieurs de la Fédération de Russie, comme l’auteur de cette attaque ; l’Union européenne a manifesté sa solidarité sans confirmer l’attribution.

Une autre affaire d’espionnage nous a beaucoup occupés : les failles dans le logiciel de messagerie Microsoft Exchange, discrètement exploitées avant d’être révélées par des attaquants qui ont cherché à exploiter un maximum de victimes. Pendant quelques jours, on a assisté à des vagues d’attaques tous azimuts, en France comme ailleurs, sachant que ce que l’on trouve dans les messageries est toujours très intéressant en termes de renseignement. Ni la France ni l’Union européenne n’ont attribué cette attaque, mais les États-Unis ont désigné la Chine. Cette affaire a conduit l’ANSSI à mener des tests de vulnérabilité ; ils ont révélé qu’environ 15 000 serveurs auraient pu être exploités. Cela ne signifie pas que tous l’ont été mais que des failles de sécurité non corrigées permettaient l’accès aux appareils de très nombreuses entreprises et de l’administration.

Le troisième phénomène qui nous mobilise est le sabotage, c’est-à-dire la cybermenace sous l’angle militaire destructif. Les cas de ce type sont heureusement plus rares parce que les opportunités sont moins nombreuses et que ces attaques coûtent cher. Dans ce domaine, on a assisté, l’été dernier, à un jeu de ping-pong entre l’Iran et Israël, Israël déclarant être ciblé sur la distribution d’eau potable, secteur extrêmement critique. Et, pour la première fois, nous avons médiatisé une attaque menée en France, semblable à celle qui a visé SolarWinds mais cette fois à des fins de destruction. Nous avons identifié un attaquant qui s’était positionné en agent dormant dans les réseaux d’une vingtaine de victimes en France, profitant de portes dérobées utilisant le mode opératoire Sandworm, associé en sources ouvertes au GRU, la direction générale des renseignements de l’état-major des forces armées de la Fédération de Russie. Ainsi, au moyen de cyberattaques discrètes et sophistiquées, nos adversaires semblent préparer les conflits de demain, qui seront également des conflits numériques. Nous devons nous y préparer en protégeant impérativement ce qui doit l’être.

L’intensité de la menace et le nombre d’attaques ne font que croître – et encore ne parlons-nous de ce que nous voyons. Face à cela, la réaction de l’État, et plus généralement de l’écosystème cyber, est essentielle. Au fil des ans nous avons construit différents dispositifs, dont la chaîne C4. Nous avions pris garde, lors de la création de l’ANSSI, de séparer des fonctions qui me paraissaient incompatibles, du moins dans le modèle français. Aussi l’Agence a-t-elle pour missions l’anticipation, la prévention, la détection et la réponse à incident, mais elle ne joue aucun rôle en matière de renseignement ni d’attaque. Cela étant dit, si l’on veut être efficace, il est impératif que tous les acteurs se parlent. Tel est l’objet du C4 TECHOPS, qui rassemble la DGSE, la DGSI, le commandement de la cyberdéfense (COMCYBER), la direction générale de l’armement et l’ANSSI. Ces entités partagent en permanence analyse de la menace et qualification des incidents, de manière que ces informations ne se perdent pas entre les services. Des années ont été nécessaires à la construction de cette communauté de confiance, entre des acteurs de nature différente, qui composent une sorte de « premier cercle cyber ».

L'efficacité de ce dispositif sera encore renforcée si l'article 17 du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement est adopté ; il prévoit que le procureur de la République de Paris peut communiquer à certains services de l'État des éléments nécessaires à l'exercice de leur mission en matière de sécurité et de défense des systèmes d'information. Il ne s'agit pas de forcer la main du monde judiciaire, avec lequel nous travaillons déjà très bien – notamment avec la section J3 du Parquet de Paris, spécialisée dans le traitement des questions de cybercriminalité, qui sait que l'intérêt général demande la transmission d'informations dans le respect de la loi. Mais cette évolution législative assiéra notre confort juridique et assurera que les services concernés ne travailleront pas en silo, au risque d'une étanchéité inefficace.

Présidé par le SGDSN, le C4 STRAT est le niveau stratégique de la chaîne C4. Dans cette enceinte de niveau secret défense, le Quai d'Orsay, la Chancellerie et Bercy s'adjoignent aux services déjà cités. On y définit pour les proposer aux autorités politiques les stratégies de réponse les plus adaptées aux grandes menaces cyber : leviers diplomatiques, leviers techniques, contre-attaques, sanctions économiques… tout est permis pour répondre aux agressions provenant la plupart du temps de grands États. Les scénarios de réponse élaborés au sein du C4 STRAT sont traités en Conseil de défense et de sécurité nationale. Il est parfois difficile de trouver des réponses pleinement efficaces, notamment face à certains agresseurs tels que ceux que j'ai cités précédemment, mais nous progressons.

Par ailleurs, j'indique que 136 millions d'euros sont prévus dans le plan de relance pour élever le niveau de sécurité du secteur public en France. La gestion de cette enveloppe est confiée à l'ANSSI ; c'est un fort montant pour une Agence qui, mis à part sa masse salariale et certains frais annexes, dispose d'un budget annuel de 20 millions d'euros. Ces fonds nous servent à aider ceux qui en ont besoin par le biais d'audits que nous finançons, qu'il s'agisse d'hôpitaux, de collectivités locales ou de certains services publics qui ont compris l'enjeu de la cybersécurité mais qui ne savent pas comment procéder. Un audit réalisé par des acteurs privés leur propose un plan de remédiation ordonné. Dire « Vous avez un problème de sécurité, on vous donne 100 000 euros, résolvez-le », cela ne marche pas, parce que les organisations ne savent pas comment dépenser cet argent. En orientant l'action, l'audit met efficacement le pied à l'étrier. Nous prévoyons d'affecter 60 millions d'euros à cette fin aux collectivités locales – nous avons déjà plusieurs centaines de candidats – et 25 millions aux hôpitaux. Nous ne prétendons pas sécuriser les 4 000 établissements de santé de France, mais l'objectif est bien de remettre le pied à l'étrier des hôpitaux d'une certaine taille.

L'enveloppe prévue dans le plan de relance nous permettra aussi de développer des centres d'alerte régionaux pour compléter la couverture des victimes potentielles. Un million d'euros y sera consacré pour aider au lancement du dispositif, puis il reviendra aux acteurs locaux de prendre la suite. Nous allons former les gens appelés à travailler dans ces centres régionaux, et nous le ferons aussi pour certains secteurs d'activité. Nous venons ainsi d'ouvrir un centre d'alerte destiné au monde maritime car si autorités portuaires et transporteurs ont des intérêts de protection communs, ils n'y travaillent pas forcément ensemble. Une sorte de communauté de cybersécurité maritime émergera ainsi. Nous nous sommes inspirés des grandes banques qui, toutes concurrentes qu'elles soient, ont compris que leur intérêt est de partager les informations en matière de cybersécurité. L'ANSSI au travers du plan de relance joue un rôle incitatif, nous pouvons allouer un peu d'argent pour initier le mouvement, nous formons des gens puis nous animons la communauté des centres opérationnels pour que l'information circule vite et de la manière la plus efficace possible.

Enfin, nous proposerons, en nous inspirant des Britanniques, experts en cette matière, des services automatisés de cyberdéfense – capacités d'audit par exemple –, qui contribueront également à élever le niveau de sécurité.

Alors que la présidence française de l'Union se profile, trois sujets sont à l'ordre du jour à l'échelle européenne. Sur le plan réglementaire, la directive NIS relative à la sécurité des réseaux d'information est en cours de révision ; il s'agit de la renforcer en nous donnant un levier réglementaire sur les entreprises de services du numérique (ESN). Toute attaque d'une ESN a un effet systémique catastrophique, l'attaquant ayant un accès direct à tous les clients. Nous devons donc pouvoir coopérer, de manière un peu forcée, avec toutes les ESN, et surtout placer la barre communautaire suffisamment haut. Nous travaillons très bien avec les ESN françaises – Capgemini, Atos, Sopra, Steria – mais elles expliquent que la sécurité informatique ne peut être offerte, car elle a un coût. Aussi longtemps que ce volet ne sera pas rendu obligatoire dans les contrats, les entreprises qui n'incluront pas ce coût, soit 10 % des budgets informatiques, dans leur réponse aux appels d'offres gagneront les marchés, car elles seront moins-disantes. Il importe donc de réviser la directive NIS en ce sens, et nous nous féliciterons que la révision aboutisse lors de la présidence française de l'Union.

D'autre part, les États européens ont développé leurs capacités, qui fonctionnent désormais en réseau, et la France est très active dans l'animation de ces réseaux à l'échelle européenne. Mais il existe un point faible, les institutions européennes elles-mêmes, cibles évidentes, surtout en matière d'espionnage, y compris par nos alliés. Nous devons donc parvenir à élever le niveau de sécurisation à l'échelle européenne, et la France a un rôle moteur à jouer en ce domaine. Reste enfin à traiter la question de la solidarité : aujourd'hui, les procédures d'assistance à un État membre qui demanderait de l'aide en cas de cyber-attaque ne sont pas organisées. Nous souhaitons donc que soit évoquée au niveau ministériel pendant la présidence française de l'Union, la manière d'utiliser des ressources européennes, publiques mais également privées, quand un État-membre est la cible de fortes attaques.

Je ne finirai pas sans faire un peu de publicité au Campus Cyber qui ouvrira à la fin de l'année dans une tour à La Défense, offrant des conditions de travail attrayantes à de nombreux acteurs du secteur public et du secteur privé appelés à collaborer dans le domaine de la cybersécurité. Y seront rassemblés des industriels de la cybersécurité et du numérique de toutes tailles, des start-up, des chercheurs, des formateurs et des services de l'État tels que le nôtre, afin que tous travaillent réellement ensemble. Inspiré en partie de ce qui existe à Be'er Sheva, en Israël, Le Campus Cyber doit permettre de passer au niveau supérieur dans la coopération ; il fonctionnera en réseau avec d'autres campus, dont le pôle de cyberdéfense de Rennes qui agit sous l'impulsion du ministère des armées.

Enfin, je saisis cette occasion pour vous dire qu'il manque à l'ANSSI un pouvoir d'injonction. Actuellement, ce que nous disons est considéré comme une information parmi d'autres. Après avoir détecté 15 000 attaques possibles sur les serveurs de Microsoft Exchange, nous avons prévenu les quelques milliers de victimes potentielles que nous avons réussi à joindre ; 3 % d'entre elles seulement nous ont répondu. Il est inacceptable que des gens auxquels on dit : « Vous êtes assis sur une bombe » ne traitent pas la question. Notre homologue américain dispose d'un pouvoir d'injonction, récemment durci ; quand une faille du type de celle qui a affecté Microsoft Exchange est détectée, il écrit à toutes les agences fédérales en leur donnant 48 heures pour les corriger, après quoi la sanction tombe. Une disposition légale donnant à l'ANSSI un pouvoir d'injonction serait une étape supplémentaire

dans le développement de notre écosystème cyber et motiverait davantage encore ceux qui bénéficient de nos services. Tout cela doit rester évidemment bienveillant et dans une logique d'accompagnement de la montée en compétences, mais il en va de la cybersécurité nationale.

Mme Françoise Ballet-Blu. Votre présentation inquiétante mais passionnante nous a permis de prendre conscience des enjeux et de l'ampleur de votre tâche. Lutte contre la cyber-menace et protection des systèmes d'information sont une des priorités de la loi de programmation militaire ; l'espace, la cyberdéfense et le renseignement ont été dotés de budgets importants dans la loi de finances pour 2021. La stratégie gouvernementale vise à accompagner la transition numérique de la Nation, à soutenir les entreprises du numérique et à défendre les intérêts fondamentaux du pays. Les attaques mettant à mal la sécurité de nos concitoyens et notre souveraineté se multiplient ; peut-on identifier leur origine géographique ? De quels leviers de négociation ou de pression la France dispose-t-elle pour limiter au maximum ces très graves atteintes à ses intérêts nationaux ?

M. Philippe Meyer. La compétition en vue du contrôle des systèmes d'information fait s'affronter des pays dont les intentions ne sont pas vraiment pacifiques. Disposez-vous des moyens techniques et humains nécessaires et suffisants pour assurer vos missions de protection de nos installations, de nos institutions, de notre défense, de notre économie, de nos collectivités et de nos hôpitaux ? L'installation prévue dans le domaine de la 5G de l'entreprise chinoise Huawei à Brumath, à proximité d'installations militaires très sensibles, suscite débats et inquiétudes. Huawei ayant espionné il y a quelques mois les conversations de l'ancien premier ministre néerlandais, n'est-ce pas faire entrer le loup dans la bergerie ? Les entreprises de ce type et celle-ci en particulier sont-elles l'objet d'une surveillance particulière ?

M. Jean-Pierre Cubertafon. L'ANSSI veut contribuer à l'élaboration d'un écosystème de cybersécurité toujours plus performant par une coopération structurée efficace avec tous les acteurs concernés par ces questions. À ce jour, la collaboration est-elle satisfaisante entre l'Agence et les collectivités territoriales ? Dans le cadre de l'actualisation de la LPM, souhaitez-vous l'évolution des moyens permettant cette coopération ? Je signale pour finir qu'en Nouvelle-Aquitaine, Pôle emploi a créé une mission sur la cybersécurité dans une démarche de sensibilisation des demandeurs d'emploi et des entreprises, en partenariat avec la gendarmerie et la police – j'en parle d'autant plus volontiers que mon fils s'en occupe… *(Sourires)*

M. Jean-Charles Larsonneur. Je vous adresse, à vous et à vos équipes, mes félicitations pour votre contribution quotidienne à l'établissement d'un écosystème de cybersécurité plus résilient et je vous remercie d'avoir mentionné la cybersécurité maritime ; les élus brestois sont très impliqués dans ce projet. Le groupe Agir Ensemble soutiendra votre demande de pouvoir d'injonction.

La souveraineté numérique française est liée à notre capacité à maîtriser la technologie du cloud et, en ce domaine, les entreprises américaines prédominent. Avec la stratégie nationale « cloud de confiance », l'ANSSI sera chargée de certifier les prestataires sur lesquels entreprises, administrations et citoyens pourront se reposer. Au nombre des conditions nécessaires à la certification, les géants américains tels qu'Amazon Web Services devront commercialiser leur offre sous licence accordée à des fournisseurs français ; cela suffit-il à s'affranchir de l'application extraterritoriale du droit américain, dont le célèbre

cloud Act ? D'autre part, nous devons investir le domaine de la cryptologie pour protéger nos transmissions. Au niveau européen, un consortium d'entreprises piloté par Airbus Defence and Space et dans lequel figure Thales est chargé de concevoir le futur réseau européen de communication protégé par les technologies quantiques dit Euro QCI. J'ai noté aussi que le premier financement du Fonds Innovation Défense a été destiné, à hauteur de 25 millions d'euros, à Pasqal, start-up française spécialisée en ce domaine. Mais alors, quelles solutions doivent être étudiées à l'échelle nationale, et quelles solutions au niveau européen ? Question subsidiaire : une partie de l'enveloppe de 136 millions d'euros du plan de relance est-elle allouée à la technologie quantique de cryptologie ?

M. Yannick Favennec-Bécot. En 2020, le nombre de cyber-attaques visant les TPE et les PME a au moins quadruplé. Un ancien secrétaire d'État au numérique l'a expliqué : si 25 000 TPE et PME tombent le même jour, l'État français lui-même sera menacé. Dans ces conditions, il est urgent que nos entreprises modifient leurs habitudes et durcissent leur système de sécurité. Que pensez-vous de la proposition de l'Institut Montaigne visant à mobiliser les réseaux de métiers du chiffre – experts-comptables et commissaires aux comptes – afin de réaliser un diagnostic annuel de la sécurité informatique des entreprises avec un cahier des charges minimum ? Quel avis portez-vous sur l'idée de créer un système de notation cyber des entreprises, sur le modèle de la notation de la Banque de France ?

Mme Carole Bureau-Bonnard. Vous l'avez souligné, la nécessité de se protéger des cyber-attaques n'est pas encore suffisamment perçue et vos recommandations en ce sens ne reçoivent pas toujours l'attention nécessaire ; comment améliorer cette situation ? Sur un autre plan, la coordination entre les services français et leurs homologues européens est-elle satisfaisante ou doit-elle être renforcée, et de quelle manière ? Enfin, intégrez-vous dans votre action le respect des normes environnementales européennes ?

M. Guillaume Poupard. La situation actuelle de l'ANSSI me satisfait. Notre effectif croît de 40 à 50 ETP par an. Cela signifie que je dois recruter quelque 150 personnes chaque année pour faire face aux départs naturels : beaucoup de nos salariés sont des jeunes gens embauchés sous contrat qui n'ont pas vocation à rester à l'Agence jusqu'à la retraite. Notre effectif devrait être de 750 agents à l'horizon 2025, ce qui donne à l'ANSSI les moyens de son action, étant entendu qu'elle ne fera pas tout à elle seule : notre mission est de contribuer à la cybersécurité mais la question concerne la collectivité nationale dans son ensemble. Notre rôle est de porter des réglementations et de répondre aux incidents en relation avec nos partenaires nationaux. Nous devons donc maintenir l'équilibre atteint. Si notre effectif n'augmentait pas chaque année dans les proportions dites, je serais contraint de faire des choix difficiles et d'abandonner des actions utiles. Mais si l'on me disait que notre mission est d'une importance telle que l'on va affecter chaque année à l'Agence de 100 à 150 ETP supplémentaires, je serais mal à l'aise parce que je ne suis pas certain qu'ils seraient utilisés efficacement. La protection contre la cybermenace repose aussi sur le secteur du renseignement, lequel dispose de moyens considérables parce qu'il lui est beaucoup plus difficile qu'à nous de se reporter sur des acteurs privés. La LPM fait état de forts besoins pour le cyber et à mon sens, sans être un va-t-en-guerre, la priorité est plutôt à l'offensif. En résumé, pour l'ANSSI, un effectif de quelque 750 personnes à terme, ou peut-être un peu plus, me semble judicieux. Viser un personnel de 2 000 à 3 000 agents conduirait probablement à déresponsabiliser ceux que nous voulons au contraire mobiliser.

Les questions relatives à Huawei sont complexes. L'essentiel a été fait par la loi du 1er août 2019 sur le contrôle des réseaux 5G, aux termes de laquelle tout opérateur voulant installer une antenne en France doit avoir l'autorisation du Premier ministre. Nous utilisons cette disposition capitale de manière équilibrée. Ce qui est, de fait, une manière de contrôler les équipementiers chinois a été attaquée par les opérateurs, avec lesquels cinquante contentieux sont en cours. Mais le Conseil constitutionnel a validé le bien-fondé de la disposition, par laquelle on se fonde sur des questions de sécurité nationale pour autoriser ou refuser le déploiement d'un réseau, en tenant compte notamment de l'origine géographique des équipementiers. Voilà ce qui nous sauve, dans un jeu complexe avec des opérateurs qui mettent évidemment en exergue des considérations économiques : ainsi, prétendument, les installations de Huawei marcheraient mieux et coûteraient moins cher que d'autres. Mais pourquoi donc ? Il ne faut pas être naïf.

Pour autant, faut-il aller jusqu'à bannir un équipementier comme les États-Unis l'ont fait avec Huawei ? Nous ne le pensons pas, car une démarche très discutable envers une entreprise que l'on accuse de tous les maux n'est pas forcément efficace. Il n'est pas grave que Huawei implante à Paris son centre de recherche en design – au contraire, cela montre que la France attire. Quand la société installe un centre de recherches à deux pas d'ici, on peut s'interroger – et on s'interroge. Quand Huawei a décidé d'installer une usine proche de Strasbourg, différents services se sont penchés sur ce choix, sans naïveté. Je ne pense pas que cela crée un risque réel ; cela nous permet plutôt de dire que nous décidons objectivement des autorisations et des refus d'installations, sans faire une fixation sur un industriel particulier. C'est donc aussi une manière de donner des gages, dans un contexte diplomatique complexe et sujet à de nombreuses tensions. Nous devons être extrêmement vigilants, et fermes quand nous avons de bonnes raisons de l'être, mais nous ne devons pas faire de cet industriel un martyr, car nous en sortirions très probablement perdants.

Sur l'origine des cyberattaques, sujet majeur, notre doctrine, qui s'est établie au fil du temps avec la DGSE, la DGSI et le COMCYBER, est de faire autant que possible de l'imputation, en apportant aux autorités politiques un maximum d'éléments permettent de dire qui, selon nous, est derrière une attaque. Notre certitude est rarement totale, car l'analyse technique ne donne quasiment jamais de garanties. Aussi, une imputation efficace avec un haut niveau de certitude suppose du renseignement complémentaire. C'est dire que si nous voulons assurer notre souveraineté et notre autonomie sans nous limiter à croire nos alliés anglo-saxons sur parole, il nous faut une capacité de renseignement autonome dont je puis vous dire sans entrer dans le détail qu'elle progresse très nettement. Les services nous apportent de plus en plus d'éléments complémentaires qui nous permettent de déposer des dossiers solides sur le bureau de nos autorités.

Après l'imputation, acte technique, vient l'attribution, acte politique qui peut varier en fonction de la situation géopolitique ou d'autres intérêts, et qui peut être rendue publique, comme le font les Américains, ou être signalée en privé et rester secrète. Il m'arrive d'accompagner des autorités politiques dans des pays compliqués auxquels on dit : « Nous vous avons percés à jour, ce que vous faites est inacceptable ». Je ne suis pas certain que cela les terrorise, mais cela porte. Choisir un canal de communication qui n'est pas public, c'est probablement l'efficacité optimale que l'on peut atteindre. Nous nous attachons à rechercher une attribution collective, notamment à l'échelle de l'Union européenne. Une Europe forte, capable de dire à Vingt-Sept : « Ce que vous avez fait est inadmissible », c'est la voie que nous encourageons et nous en parlons beaucoup avec la Commission européenne et avec nos

partenaires européens. De là à faire suffisamment pression sur des acteurs pareils – nos alliés compris, d'ailleurs – pour parvenir à empêcher les attaques… Il ne faut pas se leurrer, nous n'avons pas de pouvoir de dissuasion. Nous pouvons nous faire respecter et élever le niveau de coût de ces attaques pour leurs auteurs, mais nous ne sommes pas en mesure de les empêcher uniquement par ces moyens de nature diplomatique.

Vous m'avez interrogé sur l'état de notre coopération avec les collectivités territoriales. Nous sommes bien reçus, mais nous avons souvent affaire à des gens qui considèrent ne pouvoir s'occuper de la cybersécurité, domaine qu'ils jugent compliqué sinon incompréhensible et n'étant pas de leur ressort. Je comprends que l'idée de devoir se prêter à cet exercice peut être perturbante mais ce qui est déjà nécessaire, comme l'a montré le cas de Marseille, le sera encore davantage avec le développement des *smart cities*. Elles sont difficiles à sécuriser et ce sont les collectivités qui les géreront ; elles ont donc un rôle à jouer. Valenciennes teste le schéma alternatif, qui est de confier la ville à un industriel, Huawei en l'espèce. Je suis contre, mais certaines collectivités l'expérimentent. C'est leur choix, mais à mon avis elles le regretteront. Ici, il s'agit d'un industriel chinois, mais serait-ce un industriel français bien sous tous rapports que le problème serait le même : on ne délègue pas la gestion d'une ville. On peut déléguer des concessions, mais les décisions restent aux collectivités. L'ANSSI s'emploie donc, comme je vous l'ai indiqué, à leur mettre le pied à l'étrier en les incitant à faire mener les audits de cybersécurité nécessaires à la mise en œuvre des plans adéquats, qu'elles devront prendre en charge, car les leviers sont à leur main.

Toutes les forces vives – la gendarmerie, la police, les réservistes, les commissaires aux comptes… – doivent contribuer à la sensibilisation. Elle doit commencer dès l'école, et l'on progresse : cette année, pour la première fois, la cybersécurité était au programme du deuxième cycle des lycées et il existe désormais une option « numérique » en classe de première. Cela permet de former les enfants en faisant passer des messages au juste niveau. Il faudra encore former des professionnels pour commencer cette sensibilisation dès le collège et, plus largement, faire de la cybersécurité une grande cause nationale, ce qui permettrait d'adresser à toute la population les messages que diffuse la plate-forme cybermalveillance.gouv.fr. L'initiative de Pôle emploi que vous avez citée, excellente, est de celles qui ont un effet d'entraînement.

Le « cloud de confiance » est un sujet compliqué. Nous avons de beaux acteurs français – OVH, Outscale, Scaleway… – qui ont une parfaite compréhension des enjeux et avec lesquels nous pouvons travailler en confiance. Mais nous n'aurons ni au niveau national ni au niveau européen à court et moyen-terme certaines offres que proposent les *hyperscaler*s américains et dont nos industriels ont besoin pour fonctionner à mesure que se développe le télétravail. Aussi, le compromis annoncé récemment par le Gouvernement consiste à autoriser les *hyperscalers* américains à opérer sous licence avec des acteurs de confiance français, après que nous aurons vérifié la sûreté technique et juridique des contrats. C'est une voie compliquée mais intéressante à tenter. L'ANSSI est très impliquée dans ce processus, puisque toute la vérification technique opérationnelle lui revient.

On doit pouvoir assurer la sécurité juridique de ces montages face à une réglementation américaine hyper-intrusive d'application extraterritoriale, mais nous n'en avons pas la certitude absolue, d'autant que nul ne sait si le *cloud Act* et le *Patriot A*ct ne seront pas suivis d'autres textes de portée encore plus large. Nous devons donc nous employer à ce que les structures portant ces offres soient juridiquement distinctes de leur maison mère.

Capgemini et Orange ont ainsi annoncé leur intention de créer une société commune, Bleu, pour commercialiser en France une offre de Microsoft. Capgemini, qui a des activités majeures aux États-Unis, ne peut proposer cette offre en son nom propre mais elle le peut à travers une filiale. Nous devrions parvenir de cette manière à un niveau suffisant de sécurité juridique avec Microsoft pour ce qui est de notre sécurité économique – nous ne procéderons pas de la même manière pour nos systèmes de défense – mais il faudra être très vigilant car le diable est dans les détails. Avec Google et Amazon nous n'y sommes pas encore et ils devront faire des efforts importants. Je pense qu'ils les feront parce qu'ils y ont un intérêt économique : ces sociétés coopèrent évidemment avec les autorités américaines quand elles le leur demandent, mais elles veulent avant tout gagner de l'argent. Elles savent que les questions d'autonomie stratégique en Europe ne seront pas abandonnées et ne veulent pas se priver de ce marché.

En matière de cryptologie, nous saurons faire évoluer les algorithmes ; c'est un gros travail. En toute franchise, je n'aurais pas forcément destiné autant d'argent à Euro QCI, mais cette décision est le fruit d'un consensus. La recherche et le développement en matière de technologies quantiques coûtent très cher et il ne faudrait pas que ce financement ait un effet d'éviction pour d'autres travaux. Il est vrai que développer la technologie quantique sera utile dans d'autres domaines, si bien que je ne sais pas mesurer exactement quel sera le retour sur investissement. En bref, le développement de cette technologie n'est pas indispensable sur le plan strictement opérationnel mais n'est pas une mauvaise idée pour autant. Rien dans l'enveloppe de 136 millions d'euros que j'ai mentionnée ne concerne le quantique : elle vise à des réalisations bien plus pragmatiques tendant à élever le niveau de sécurité assez rapidement. Il faut anticiper la menace quantique, mais ce n'est pas la priorité du plan de relance.

Lorsqu'une PME subit une cyberattaque, on est face à un triste fait divers. Si 10 000 étaient attaquées en même temps, ce qui est tout à fait possible, au-delà de l'effet économique la sécurité nationale serait effectivement en jeu. Faire participer les professionnels tels que les experts comptables et les commissaires aux comptes à la prévention de cette menace est indispensable ; eux-mêmes le disent, ajoutant que s'ils ne sont pas certains que les réseaux informatiques de leurs clients sont sains, ils ne savent pas s'ils certifient les vrais chiffres ou des chiffres manipulés par un attaquant. Mais si les gros cabinets ont déjà, en général, des activités de conseil en matière de cybersécurité, ce n'est pas le cas des petits cabinets de commissariat aux comptes : comment pourraient-ils avoir un avis légitime sur le niveau de sécurité de leurs clients ? Si obligation leur est faite, un jour, d'en donner un, ils disparaîtront. L'idée est donc bonne, mais elle peut être dangereuse pour les petits cabinets, qui doivent dans un premier temps diffuser les bonnes pratiques et procéder aux vérifications élémentaires.

L'hypothèse d'une « notation cyber » est intéressante, mais on ne sait pas encore la mettre en œuvre. Un avis étayé sur le niveau de cybersécurité d'un acteur économique suppose de s'appuyer sur un audit, procédure coûteuse, longue et lourde, alors qu'une notation doit pouvoir s'appliquer à tous. Diverses tentatives de notation ont déjà été faites, qui se sont toutes traduites par des échecs jusqu'à présent. Mais l'on y viendra car ce serait utile, comme l'est la notation financière.

Le Campus Cyber a été conçu pour assurer la communication entre les acteurs de la cybersécurité. Notre seule chance d'appartenir au cercle des pays capables de garantir leur

souveraineté numérique est d'optimiser le lien entre chercheurs, formateurs, entreprises et ministères concernés. Si chacun joue sa propre partition, cela ne marche pas. C'est une des responsabilités de l'ANSSI de porter cette conception au niveau national, et les choses se passent plutôt bien même si des progrès sont toujours possibles.

Beaucoup a été fait en matière de coopération européenne. La cybersécurité européenne se fait en trois phases et nous sommes au niveau de la troisième. En premier lieu, chaque État membre devait impérativement développer ses propres capacités. L'idée que seuls les grands pays doivent le faire et qu'ils protégeront les petits pays est mauvaise ; cela peut fonctionner dans certains domaines militaires mais pas en matière de la cybersécurité. Le développement général de ces capacités a eu lieu, notamment grâce à la directive NIS. La deuxième étape consiste à organiser ces capacités en réseau, ce qui commence à bien progresser : un réseau opérationnel est en place qui permet à l'ANSSI et à ses vingt-six homologues d'échanger en permanence des informations opérationnelles, et ce dispositif monte en puissance. L'optimum n'est pas encore atteint mais les choses fonctionnent bien, au niveau des instances de coopération techniques comme au sein du réseau stratégique CyCLONe, créé il y a deux ans avec le soutien bienveillant de la Commission européenne et de l'Agence européenne pour la cybersécurité, l'ENISA. Le troisième niveau est le déclenchement de la solidarité européenne si un État subit une cyberattaque. Nous souhaitons avancer à ce sujet pendant la présidence française de l'Union. Ce n'est pas hors de portée, mais cela suppose un niveau de confiance assez élevé car aider un État n'est pas si simple ; je suis convaincu que nous ne parviendrons à notre objectif que si nous faisons intervenir, outre des acteurs étatiques, des prestataires privés.

Sans aller jusqu'à dire qu'il n'y a pas de lien entre les missions de l'ANSSI et les questions environnementales, je ne sais pas vraiment répondre à votre question sur ce que l'Agence fait en ce domaine – pas grand-chose, en vérité. Inversement, certains s'en prennent au chiffrement parce que cela gêne les services d'enquête et de renseignement. Deux des arguments utilisés me font bondir : d'abord, que le chiffrement étant utilisé par les pédophiles, y être favorable c'est être favorable à la pédophilie, d'autre part que l'empreinte carbone du chiffrement est élevée en raison de la puissance de calcul nécessaire. Je ne suis pas certain que ce soit de bonnes raisons pour interdire le chiffrement ou en réduire l'efficacité. Que l'on commence donc par s'intéresser aux cryptomonnaies, catastrophes écologiques surtout utilisées par des criminels ou à leur bénéfice, ou par des spéculateurs.

Mme Patricia Mirallès, présidente. Monsieur le directeur général, nous vous remercions pour vos explications claires et directes.

*

* *

La séance est levée à dix-neuf heures cinq.

*

* *