ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Mardi
31 janvier 2017
Séance de 17 heures

Compte rendu n° 24

SESSION ORDINAIRE DE **2016-2017**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence
de Mme Patricia Adam,
présidente

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures.

Mme la présidente Patricia Adam. Chers collègues, nous avons déjà auditionné M. Poupard en 2013, lorsque nos réflexions sur la cybersécurité ne faisaient que commencer.

Depuis, le travail de l'Agence nationale de sécurité des systèmes d'information (ANSSI) a beaucoup avancé et nous souhaiterions faire le point. Nous avons auditionné à ce sujet le ministre de la Défense, qui s'est particulièrement impliqué dans ce domaine, et les services de son ministère. Nous avons également rencontré nos collègues d'Estonie et d'Allemagne ; ces derniers sont très sensibilisés à la question de la sécurité informatique puisque des élections législatives se dérouleront dans ce pays en septembre. Les Allemands sont particulièrement inquiets de la possibilité d'attaques informatiques en provenance de Russie, comme cela a pu se passer aux États-Unis.

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information. Il est d'usage d'évoquer l'état de la menace en introduction, mais je sais que vous commencez à très bien la connaître. Cette menace ne fait que s'accroître en quantité et en qualité, tous les indicateurs annoncent un durcissement des attaques que nous aurons à subir à l'avenir, indépendamment de la prévention et des moyens que nous pouvons déployer pour les prévenir et y réagir rapidement. Du fait de l'évolution technologique, et du fait du fonctionnement de nos sociétés, nous allons subir de plus en plus d'attaques, d'une force de plus en plus grande.

Cette menace peut être caractérisée en quelques mots. Tout d'abord, les activités cybercriminelles prennent aujourd'hui une ampleur importante. Elles touchent notre économie, nos PME et nos concitoyens. Si elles ne sont pas graves, *a priori*, en termes de sécurité nationale, elles peuvent avoir un effet systémique. Une PME touchée, c'est un fait divers ; mais si 5 % des PME françaises se retrouvent dans l'incapacité de fonctionner, cela devient une question de sécurité nationale aux incidences majeures sur l'économie et la société.

Nous observons aujourd'hui des groupes criminels de plus en plus organisés, manifestement protégés, installés parfois dans des pays très lointains, et qui gagnent des quantités d'argent absolument folles, bien supérieures aux revenus du trafic de drogue ou d'autres trafics. L'argent ainsi gagné est réinvesti, ce qui permet à ces criminels de progresser techniquement de manière extrêmement rapide.

Mme la présidente. Comment gagnent-ils de l'argent ?

M. Guillaume Poupard. Par le passé, les virus et les attaques informatiques tenaient plutôt de la revendication ou de l'exploit : des messages s'affichaient à l'écran, des sites internet étaient affectés. Aujourd'hui, les virus repèrent dans un ordinateur ou un réseau informatique les données importantes, les chiffrent de manière très robuste, et exigent une rançon des victimes pour leur rendre leurs données. Il s'agit de petites sommes, de l'ordre de 1 000 euros. Mais pour une PME, entre payer 1 000 euros et perdre toutes ses données, il n'y a pas de doute, elle va payer. Toutes ces petites sommes additionnées à l'échelle internationale représentent des volumes colossaux. L'ordre de grandeur des revenus est plutôt de l'ordre du milliard d'euros. Nous avons vu des campagnes toucher des hôpitaux ; un hôpital américain, notamment, a reconnu avoir payé 17 000 dollars. À l'échelle du budget

d’un grand hôpital, cette somme ne représente rien, et cela prouve que les victimes paient assez facilement pour récupérer leurs données. Mais dans certains cas, même après qu’elles ont payé, on ne les leur rend pas… et certaines PME mettent la clé sous la porte car elles n’arrivent plus à accéder à leurs données. Pour beaucoup de PME des nouvelles technologies, la richesse, ce sont les données, et les perdre est dramatique.

Ce type de criminalité en développement impose de trouver des moyens de protection adaptés aux PME, ce qui n’est pas forcément du ressort de l’ANSSI, de mener des actions de sensibilisation et de les convaincre d’adopter une démarche saine pour leur usage du numérique, car les conséquences peuvent être dramatiques.

Le deuxième type de menaces est très peu abordé, bien que l’ANSSI ait beaucoup de cas graves à connaître, car les victimes ne souhaitent pas communiquer ; il s’agit du vol d’informations, de l’espionnage ou de l’intelligence économique. Le scénario est toujours le même : des attaquants, plutôt compétents et organisés, entrent dans un système d’information pour y voler des informations : le contenu des messageries des dirigeants, des plans, des éléments techniques, des éléments commerciaux, des réponses à des appels d’offres. Il s’agit d’espionnage économique classique, porté à une échelle industrielle.

Les conséquences sont très graves pour les sociétés : si les bons systèmes de détection d’attaques ne sont pas installés, les entreprises risquent de s’en rendre compte seulement longtemps après. La plupart du temps, les victimes sont de grandes entreprises cotées au CAC 40, et l’espionnage est repéré deux ou trois ans plus tard. Parfois même, il n’y a plus de traces, mais on comprend que l’assaillant lisait déjà à livre ouvert dans les réseaux informatiques de la société il y a plusieurs années.

Il est très difficile d’en estimer les conséquences économiques, mais les entreprises victimes comprennent soudain pourquoi c’est un concurrent qui a gagné un marché, pourquoi un produit a été sorti qui ressemblait étrangement à leur plan secret… Dans le monde feutré du renseignement économique, on n’en parle pas, mais cette guerre souterraine fait rage, probablement avec des conséquences dramatiques sur notre économie. Là encore, donner des chiffres est difficile : on dénombre une vingtaine d’attaques majeures par an, qui donnent lieu à une opération de l’ANSSI. Cela veut dire que les conséquences sont graves, même si nous ne sommes pas en mesure de les chiffrer précisément.

Le troisième cas constitue la priorité de l’ANSSI, de par notre rattachement au Secrétaire général de la défense et de la sécurité nationale (SGDSN) : je veux parler des risques non sur les données, mais sur le fonctionnement des systèmes d’information. Aujourd’hui, tout est numérique, tout est informatisé, et ce qui ne l’est pas est en passe de le devenir. Le risque est celui d’attaques contre les secteurs d’activité d’importance vitale : les transports, l’énergie, les télécoms, la finance, les réseaux de distribution, l’industrie, la santé, etc. L’objectif de ces attaques n’est plus de voler des informations, mais de provoquer des dysfonctionnements, la destruction ou encore d’utiliser ces systèmes contre nous. La Direction générale de l’armement travaille beaucoup sur la possibilité que nos armes soient demain retournées contre nous ; un tel scénario ne peut être écarté si nous n’y prenons garde.

Ce type d’attaques s’est peu produit depuis 2013 ; nous n’en avons connu qu’une seule, contre TV5 Monde. Un acteur manifestement compétent est entré au sein du réseau informatique de TV5 Monde, a cartographié ce réseau pendant deux mois, et a déclenché

l'attaque d'un seul coup. Tous les équipements de production audiovisuelle de TV5 Monde ont été détruits en très peu de temps. Heureusement que les informaticiens de TV5 étaient sur place et ont eu le bon réflexe d'arracher tous les câbles – ce n'est pas toujours la chose à faire, ça l'était en la circonstance – ce qui a limité les conséquences. Toutefois, TV5 Monde a été entre la vie et la mort d'un point de vue informatique pendant plusieurs mois, le coût a été très élevé, et ils sont maintenant obligés de se protéger. Ce fut pour eux un véritable traumatisme.

Nous pouvons malheureusement imaginer que de tels cas se reproduisent dans de nombreux secteurs, et c'est ce que nous redoutons désormais. L'ANSSI réalise de nombreux d'audits, en coopération avec les acteurs qui prennent conscience de ce risque, et ils ne sont malheureusement pas de nature à rassurer. La plupart du temps, la conclusion de ces audits est que pénétrer les réseaux et y provoquer des dommages très graves est possible. Bien évidemment, tout n'est pas accessible au pirate du coin, mais nous n'en sommes pas moins inquiets.

D'autres attaques, qui peuvent être le fait des mêmes acteurs, portent sur le fonctionnement même de notre démocratie. L'exemple des élections américaines est intéressant de ce point de vue : c'est la première fois qu'une attaque informatique est utilisée à des fins de déstabilisation. On ne saura jamais si le résultat de l'élection a été faussé du fait de cette attaque, mais de fait, des attaquants ont volé des messages électroniques du comité démocrate et les ont publiés dans l'intention de nuire. Il est même possible que des faux aient été glissés parmi ces messages : comment prouver que ceux-ci sont faux et ceux-là vrais ? Il s'agit vraiment de guerre de l'information, aux conséquences potentielles très graves. Nous y pensons très sérieusement dans le cadre des élections qui vont avoir lieu en France, car ce qui a été perpétré aux États-Unis peut l'être de nouveau en France, par les mêmes acteurs ou par d'autres. Maintenant que l'idée a été donnée, les attaquants vont rivaliser d'idées.

Il y a donc beaucoup d'attaques, de nature variées. Parmi les cyberattaques, certaines sont des coups d'épingles, d'autres auraient des conséquences dramatiques. Il est important de chercher à s'en prémunir au mieux et, lorsqu'il est trop tard, d'être capable de réagir au plus vite pour ne pas se rendre compte que l'on s'est fait piller seulement au bout de trois ans.

Pour répondre à ces menaces, la France compte certains atouts. Sans verser dans l'autosatisfaction, nous pouvons nous féliciter de certains choix qui ont été faits par le passé, et qui se sont révélés judicieux.

Ainsi, l'organisation mise en place pour faire face à ces menaces nouvelles responsabilise l'ensemble des acteurs concernés. Aujourd'hui, beaucoup de ministères ou d'administrations peuvent jouer un rôle dans la cyberdéfense.

C'est bien évidemment le cas du ministère de la Défense pour la protection de certains systèmes très originaux tels que les systèmes d'armes ou les systèmes déployés en opérations extérieures, mais également dans le renseignement et le développement des capacités offensives.

Le ministère de l'Intérieur a également un rôle à jouer dans la lutte contre la cybercriminalité, qui reste une forme de criminalité.

Le ministère des Affaires étrangères est également concerné, car les questions diplomatiques ont une grande importance. Nous sommes amenés à traiter avec des alliés, ou avec d'autres États qui ne le sont pas, mais nous savons que tout le monde peut nous attaquer à un moment ou un autre, y compris nos alliés les plus proches. Les questions diplomatiques sont donc des enjeux de premier plan. En cas d'attaque majeure, il faut pouvoir mettre en œuvre des processus permettant la désescalade, et je ne suis pas sûr que nous en disposions aujourd'hui. À l'instar de ce qui existe dans le domaine nucléaire ou militaire, on a besoin de dispositifs permettant de se parler en temps de crise.

Le ministère des Finances a également compris qu'il était directement concerné. Aujourd'hui, notre économie est la première victime des attaques informatiques. De plus, la France est bien placée dans le domaine de la cyberindustrie, qui est pour elle une chance de développement économique.

De plus en plus d'autres ministères viennent également à ces questions. Le choix a été de laisser chacun dans son champ de responsabilité et de compétence, mais de prévoir une agence interministérielle, en l'occurrence l'ANSSI, pour coordonner ces actions, définir la stratégie pour le compte du Premier ministre et mener en propre certaines actions mutualisées. Ainsi, l'ANSSI est à la manœuvre pour tout ce qui concerne la prévention, la définition de la réglementation, la détection des attaques et la capacité à réagir pour les victimes les plus sensibles. Nous disposons des capacités opérationnelles de très haut niveau ; l'ANSSI a probablement les meilleurs experts pour porter assistance à des victimes. Cela requiert une expertise très particulière, qui est encore très rare.

Ce modèle est certainement assez bon. L'existence d'une agence interministérielle permet de ne pas être cantonné au champ de compétence d'un ministère et d'une activité donnée. Peu de pays ont adopté cette approche interministérielle. En Allemagne, le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) dépend du ministère de l'Intérieur, ce qui présente certains avantages, mais aussi beaucoup d'inconvénients.

Un autre avantage de notre organisation est la séparation très stricte entre l'attaque et la défense. Dans l'attaque, je range le renseignement et l'offensif pur. Nous avons fait le choix de séparer les deux, ce qui ne veut pas dire que nous ne savons pas nous parler, mais il faut que les missions soient claires et qu'il n'y ait pas de conflits d'intérêts. Nos alliés anglo-saxons ont fait le choix de confier la cyberdéfense à ceux qui au départ savaient faire, c'est-à-dire aux agences de renseignement technique, qui avaient été les premières à développer ces compétences. Cela pose des questions : aux États-Unis, lorsque la NSA (*National Security Agency*) arrive, on ne sait jamais vraiment qui est derrière. D'ailleurs, je pense que la NSA elle-même ne sait pas exactement quelle est sa mission… Au Royaume-Uni, la situation est proche, même si elle se clarifie. En France, nous savons que l'ANSSI a une mission purement défensive et protectrice, elle ne fait pas de renseignement ni d'attaque.

Cela n'empêche pas l'ANSSI d'échanger avec l'ensemble des services, notamment les services techniques. Nous assumons pleinement ces liens, et je suis friand de tous les éléments que les services de renseignement peuvent apporter concernant les attaques en cours ou en préparation, ou en matière d'attribution. Nous ne nous chargeons pas de l'attribution, mais les services de renseignement, en croisant différents types de sources, peuvent parfois savoir d'où viennent les attaques, même si c'est compliqué en pratique.

À mon avis, ce choix n'est pas à remettre en cause. Je suis évidemment juge et partie, mais je crois c'est une force de notre modèle d'assigner des missions claires à chacun et de permettre une collaboration vraiment efficace avec les autres entités.

Notre autre chance est d'avoir décidé très tôt qu'au vu de l'importance de la cybersécurité, il n'était plus possible de se contenter de donner de bons conseils. Les bons conseils trouvent leurs limites, notamment vis-à-vis des grands acteurs économiques, car il y a toujours mieux à faire avec l'argent. Les investissements en cybersécurité ne sont pas directement productifs ; tant que c'est une option, il est tentant de les reporter à l'année suivante. La France a fait le choix, qui s'est traduit dans la loi de programmation militaire de décembre 2013, de faire de la cybersécurité une obligation pour les opérateurs d'importance vitale. En 2013, mon prédécesseur était tenu de prendre beaucoup plus de précautions oratoires… Il a fallu deux ans de dialogue avec les opérateurs d'importance vitale – on en compte deux cent trente, parmi les acteurs les plus sensibles pour la sécurité de la nation – pour nous mettre d'accord. Mais le caractère obligatoire a été un moyen formidable de discuter avec ces acteurs.

Aujourd'hui, l'article 22 de la loi de programmation militaire nous permet d'imposer des mesures de sécurité qui placent les opérateurs d'importance vitale à un niveau de cybersécurité assez inédit en France ou à l'étranger. Au lancement de cette mesure, nos partenaires nous disaient que c'était la bonne manière de faire, mais qu'elle ne marcherait jamais, car les lobbies et les industriels allaient tout bloquer. Les Américains avaient déjà tenté une démarche similaire, mais les lobbies avaient gagné et rejeté cette approche réglementaire au profit des *best practices.* Les Allemands aussi ont trouvé que ce que nous faisions était intéressant, mais que ce n'était pas possible chez eux, et les Britanniques de même. De fait, tous se sont rendu compte que cette solution fonctionnait, et leur attitude est en train de changer. En Allemagne, une loi similaire à la nôtre permet d'imposer la sécurité aux grands opérateurs, mais de manière plus cloisonnée. Surtout, en Europe, la directive *Network and Information Security* (NIS), sur la sécurité des réseaux, reprend ces idées. Ce n'est pas le fruit du hasard : nous avons beaucoup discuté avec la Commission européenne, qui était très intéressée par ces questions.

Identifier des acteurs critiques et leur imposer la sécurité va devenir la règle en Europe. Ce sera le cas lorsque la directive sera transposée partout, en mai 2018. Cela n'empêchera pas les attaques, mais nous avons enclenché une dynamique positive, permise en France par cet article 22 de la loi de programmation militaire.

D'autres articles importants figurent dans cette loi. Nous avons pris soin de bien profiter de tout ce que nous permettait ce texte, notamment en prenant toutes les mesures réglementaires d'application. Ainsi, l'article 21 nous permet une défense active : en cas d'attaques, différents services, dont l'ANSSI, ont le droit de se connecter aux machines qui nous attaquent. Dans beaucoup de pays, cette exception aux règles existantes pour empêcher les attaques informatiques est impossible. D'autres éléments nous permettent de mener une cyberdéfense efficace, sans léser personne.

Après avoir beaucoup travaillé au niveau national, nous travaillons au niveau européen. Les grands acteurs ne sont pas français, mais au minimum de taille européenne, et ils craignent que des règles contradictoires soient édictées dans les différents pays, ce que personne ne souhaite. La directive NIS va aider à harmoniser les législations par-delà les

frontières, qui n'existent plus dans le domaine numérique. Plus généralement, il est nécessaire de disposer d'une industrie européenne dans le domaine de la cybersécurité. Elle est encore très segmentée par pays, voire complètement inexistante dans certains pays. Pour développer de tels acteurs au niveau européen, nous avons travaillé avec la Commission à la mise en place d'un partenariat public-privé permettant de flécher des fonds de recherche européenne – le programme Horizon 2020 – afin de promouvoir la recherche et le développement dans le domaine de la cybersécurité. Il est nécessaire de mettre en place une telle industrie pour développer l'autonomie stratégique européenne – manière diplomatique de dire que nous ne voulons pas dépendre totalement de nos alliés américains en termes de solutions de sécurité.

Une réflexion sur le droit international et la cybersécurité est en cours. Des réflexions ont été développées, principalement dans le domaine militaire, pour savoir comment faire la guerre dans le cyberespace. Cette question a notamment été portée par les Estoniens dans le centre d'excellence de Tallinn. Le manuel de Tallinn commence à codifier le droit de la guerre dans le cyberespace, mais il est aussi important de se demander comment faire la paix dans le cyberespace, comment y garantir une stabilité, quel droit international y appliquer. De nombreuses questions sont soulevées, car des notions qui nous paraissent évidentes doivent être redéfinies pour s'appliquer au monde numérique.

Ces questions seront abordées lors d'un grand colloque international à l'UNESCO au début du mois d'avril, de manière à ce que les différents grands pays – États-Unis, Chine, Russie - puissent venir parler de stabilité dans le cyberespace. Nous préparons ces travaux avec des juristes qui réfléchissent à la redéfinition des notions. Il faut éviter que le cyberespace de demain ne se transforme en un Far West où tout le monde porterait un colt à la ceinture, mais sans que l'on puisse trouver un *smoking gun* ; ce colt-là ne laisserait s'échapper aucune fumée trahissant son usage… Voilà le risque qui menace le cyberespace si l'on laisse les acteurs privés se faire justice eux-mêmes ou y défendre leurs intérêts. Si l'ensemble des acteurs privés se mettait à se comporter ainsi, nous connaîtrions un chaos numérique extrêmement inquiétant pour le développement numérique, qui reste le sens de l'histoire.

Mme la présidente. L'amiral Coustillière était lui aussi venu nous exposer ce qui pouvait militairement se passer dans le cyberespace.

M. Jean-Jacques Candelier. L'acquisition de nos logiciels nous inféode à Cisco, arrière-boutique de la NSA, ce qui m'inquiète. Pouvez-vous nous rassurer à ce propos ?

M. Olivier Audibert Troin. Vous avez évoqué, à juste titre, les grandes entreprises, mais notre système économique repose avant tout sur la richesse de nos PME. Si les grandes entreprises et les grands services de l'État ont les moyens financiers pour se prémunir de ces cyberattaques, les PME en manquent. Selon vous, peut-on envisager un fonds d'État spécifiquement dédié pour aider les entreprises à se protéger de ces cyberattaques ? Il pourrait être prélevé sur le « matelas » de 50 milliards d'euros qui dort dans les organismes de formation.

Pour ce qui est de la formation, notre pays est-il en retard pour inculquer l'importance de la cyberdéfense aux futurs dirigeants d'entreprises ?

M. Philippe Vitel. Je tiens d'abord à dire que je suis admiratif de la manière dont nous avons pris en compte cette problématique en France. J'ai eu l'occasion de le faire savoir hors de nos frontières, puisque j'ai commis un rapport sur ce sujet pour l'assemblée

parlementaire de l'OTAN. Nous sommes en pointe, et nous devons nous donner les moyens d'y rester.

Nous devons cette avance à quatre facteurs : tout d'abord, l'approche interministérielle, qui nous permet d'être beaucoup plus efficaces que nos alliés ; nous avons aussi été parmi les premiers à nous doter d'une stratégie nationale de cybersécurité ; les premiers à mettre en place les outils de secours, que l'on appelle les *computer emergency readiness team*, dont tout pays devrait aujourd'hui disposer ; et nous avons consacré les moyens financiers et humains nécessaires.

Mes inquiétudes portent sur les PME, en particulier dans le domaine de la défense. Je suis conseiller régional chargé des relations entre la défense et la région. Des opérations d'intérêt régional sont mises en place pour l'industrie maritime et navale. Dans le cadre de la loi NOTRe, peut-on créer des fonds de financement décentralisés pour aider les PME à se doter de véritables moyens de protection ? L'ANSSI est-elle prête à travailler avec les régions pour mettre en place de tels dispositifs ?

Les PME doivent prendre conscience de l'importance de la sécurité, et ce travail doit être réalisé en amont : dans les pépinières d'entreprises, dans les écoles d'ingénieurs, pour que ces jeunes innovateurs prennent conscience du danger qu'ils courent dès qu'ils fixent leurs innovations sur un support numérique.

Mme Geneviève Gosselin-Fleury. Pouvez-vous préciser les missions et le fonctionnement de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ?

Mme Virginie Duby-Muller. À l'occasion du forum international de la cybersécurité (FIC) qui s'est tenu à Lille les 24 et 25 janvier, vous avez annoncé la création du dispositif national d'assistance aux victimes d'actes de cybermalveillance, baptisé ACYMA. Pouvez-vous nous en dire plus ? Comment fonctionnera la plateforme en ligne ? Quelle sera la nature des interventions de l'ANSSI sur ce sujet ?

Nous le savons, aucune structure n'est à l'abri d'intrusions pouvant compromettre son fonctionnement : le phénomène du *hacking* a visé des multinationales, mais aussi des États. Sommes-nous assez protégés contre une cyberattaque ? Pensez-vous que nos lois sont suffisamment adaptées à la cyberdéfense ?

Vous vous êtes prononcé le 18 janvier dernier, lors d'une audition devant la commission des Lois à l'Assemblée nationale, contre le vote électronique. Ne disposons-nous pas de moyens suffisants pour encadrer le vote en ligne et lutter contre les potentielles cyberattaques ? Qu'en est-il des machines à voter ? À l'heure où le numérique bouleverse notre société, pensez-vous que nous pourrons résister longtemps à cette évolution ?

Plus globalement, les cyberattaques étaient jusqu'à présent principalement motivées par l'espionnage économique. Elles visent maintenant les États, et pourraient donc, à l'avenir, tendre à déstabiliser la France, comme vous l'expliquiez lors de votre audition au Sénat. Vous évoquiez d'autres menaces telles que la destruction de fichiers par une organisation ou un pays étranger. Vos propos rappellent ainsi les soupçons pesant sur les dernières élections présidentielles américaines. Pensez-vous que des faits similaires pourraient affecter les

prochaines élections en France ? Qu'a prévu l'ANSSI pour garantir le respect du vote des citoyens et pour parer à d'éventuelles cyberattaques ?

Depuis la loi pour une République numérique, dite loi Lemaire, quiconque peut désormais signaler à l'ANSSI l'existence de failles de sécurité en étant assuré que cette information ne fera pas l'objet d'une transmission automatique au parquet. Quel premier bilan tirez-vous de cette nouvelle mesure ?

Enfin, pouvez-vous faire un point sur la coopération européenne en matière de cybersurveillance et de lutte contre les cyberattaques ? Un renforcement de la coopération est-il envisagé ?

M. Guillaume Poupard. Je vous remercie pour ces questions très complètes.

S'agissant de la dépendance à l'égard des logiciels et des matériels, il n'est plus raisonnable d'imaginer que nous sommes capables de les fabriquer en France avec des industriels de confiance ; nous en avons fait notre deuil depuis très longtemps, y compris pour des applications très sensibles dans le domaine de l'armement et de la défense.

Il nous faut donc répondre à la question suivante : comment peut-on aboutir à des systèmes sûrs sans pour autant en maîtriser tous les constituants ? Lorsque l'exercice est mal fait, le résultat est catastrophique, c'est évident, et on se retrouve dépendants, à la merci de ceux qui nous fournissent les systèmes. Vous avez cité Cisco, mais ce n'est malheureusement qu'un exemple. Quand ce n'est pas américain, cela vient d'autres pays.

Comment peut-on, malgré cela, construire des systèmes qui vont être globalement sûrs, en battant en brèche l'idée encore répandue selon laquelle la sécurité d'un système est la sécurité du maillon le plus faible – ce n'est heureusement pas le cas – ? Nous préconisons une démarche par l'architecture. Il est important d'intégrer les contraintes liées à la cybersécurité dans la conception même des produits – un avion, un bateau ou n'importe quel système d'arme. Ensuite, le travail consiste à assembler des briques dans lesquelles on ne peut pas forcément placer notre confiance – il est très difficile de les développer dans des conditions économiques viables –, des briques qui doivent être fabriquées par des personnes un peu plus dignes de confiance – des industriels européens, voire français – et des briques tellement sensibles qu'on ne veut pas les confier à un industriel, mais les conserver à un niveau étatique afin d'avoir la main dessus – je pense notamment aux algorithmes cryptographiques qui sont intégralement conçus pour les besoins de la défense nationale par la DGA dans le centre de Bruz et qui sont évalués par le laboratoire de cryptographie de l'ANSSI ; à aucun moment, il n'est fait appel à quelqu'un d'extérieur à ce très petit cercle afin de garantir une confiance absolue ; nous sommes extrêmement vigilants sur les personnes et sur la sécurité qui les entoure.

C'est ce chemin très étroit que nous devons suivre : être capable de développer les briques « souveraines » et de les assembler avec des briques moins maîtrisées de manière à ce que l'ensemble du système devienne maîtrisé. J'ai la prétention de penser que c'est le cas aujourd'hui – les systèmes d'arme sont plutôt de bons exemples. Il en va de même pour les réseaux informatiques plus classiques, le travail bien fait assure une maîtrise qui permet de se protéger contre les risques identifiés.

Ma principale crainte concerne ce que l'on appelle les systèmes industriels. Je pense à l'informatique enfouie dans les entreprises et les industries et au numérique qui n'a pas été pensé en imaginant des attaques un jour. Il faut donc effectuer un travail de rattrapage. Nous le faisons notamment avec les équipementiers de manière à intégrer de la sécurité dans leurs systèmes et à vérifier cette sécurité. Nous évaluons et nous qualifions aujourd'hui des automates industriels – les premiers l'ont été il y a six mois – afin de pouvoir s'appuyer sur des briques de confiance qui pourront ensuite être intégrées dans des architectures capables de se protéger.

Tel est le chemin, je ne dis pas qu'il est confortable. Nous avons encore la prétention de penser que nous pouvons trouver un compromis – on n'aime pas ce terme dans le domaine de la sécurité – pour nous prémunir contre les risques en utilisant des systèmes à un coût acceptable.

Je me méfie toujours des débats un peu rapides. Sur la question des systèmes d'exploitation souverains, quand bien même nous disposerions d'un tel système – ce que nous n'avons pas forcément en France aujourd'hui ou pas facilement disponible –, la question du matériel et des logiciels qui l'entourent resterait posée. Si on se polarise sur une brique, cela ne fonctionne pas ; il faut une démarche d'ensemble sur l'architecture et le système.

Concernant les PME, les solutions qui marchent pour les grands groupes ne sont pas celles qui marchent pour les PME. C'est une trivialité que de le dire. L'article 22 de la loi de programmation militaire, qui impose aux opérateurs d'importance vitale de renforcer la sécurité de leurs systèmes d'information, vise très clairement les grandes structures, organisées, avec des moyens – même si elles se plaignent de leur insuffisance –, qui possèdent un service informatique, des responsables de la sécurité et une gouvernance adaptée. Pour les PME, cela ne fonctionne pas. Je suis convaincu que, pour la très grande majorité des PME, la sécurité doit être quasiment transparente. Le *cloud computing*, c'est le sens de l'histoire. Profitons de cette fenêtre de tir un peu étroite qu'offre le *cloud computing* même s'il a été beaucoup décrié pour ses failles au regard de la sécurité. Il s'agit de confier ses données, ses ordinateurs à des tiers qu'on connaît mal finalement. Mais, si le *cloud computing* est géré par des prestataires qui sont dignes de confiance et qui mettent en place des règles de sécurité, on peut espérer que les PME, en même temps qu'elles vont sous-traiter leur informatique, vont sous-traiter leur sécurité informatique. Cela me paraît être la seule voie possible. Les PME ont déjà du mal à gérer l'informatique – on connaît le cas du dirigeant de PME qui s'occupe de l'informatique le week-end quand il lui reste deux heures –, ce n'est pas raisonnable de leur demander de prendre en charge la cybersécurité. Par contre, si l'abonnement informatique inclut la sécurité de manière quasiment automatique, peut-être pour un petit supplément financier qui doit être acceptable, c'est viable. Il nous reste donc deux choses à faire : d'abord, s'assurer que les prestataires de *cloud computing* sont des prestataires de confiance. Pour ce faire, nous avons développé un programme d'évaluation et de qualification de ces derniers – les premiers sont en train d'être labellisés en ce moment. Nous pourrons dire aux PME mais aussi aux grands groupes : si vous travaillez avec ces prestataires labellisés, nous vous garantissons, au nom du Premier ministre – ce ne sont pas des certificats en l'air –, après un vrai travail d'évaluation que le niveau de sécurité et la confiance sont suffisants.

M. Olivier Audibert Troin. Quelle est la nature de la garantie que vous apportez ?

M. Guillaume Poupard. Nous établissons un référentiel public, qui comporte toutes les règles de sécurité que nous souhaitons voir appliquées. Des laboratoires indépendants, agréés par l'ANSSI, soumettent le prestataire à une évaluation fondée sur ce référentiel, et vérifient que toutes les règles sont effectivement appliquées. Nous nous assurons que le travail a été bien fait et nous certifions – je signe au nom du Premier ministre – que le produit est au bon niveau de qualité en termes de sécurité. Ce que nous faisons depuis très longtemps pour les produits, nous le faisons aujourd'hui pour les services, notamment le *cloud computing*. C'est la voie qui nous semble la plus raisonnable.

Nous conseillons aux PME de choisir ces prestataires – nous ne nous prononçons pas sur ceux que nous n'avons pas évalués. Si c'est un peu plus cher, c'est probablement normal car qui dit sécurité, dit prestations supplémentaires, matériels supplémentaires, travail supplémentaire – le service est supérieur. Ensuite, il reste aux entreprises à appliquer des règles de sécurité assez élémentaires – faire attention aux mots de passe, aux téléphones portables, aux clés USB –, ce que Patrick Pailloux a appelé l'hygiène informatique et qui reste ô combien d'actualité. Un patron de PME peut comprendre cela aisément.

Parallèlement, nous encourageons les industriels à développer des offres couplées, notamment ce qu'on appelle les « box PME ». De nombreux foyers sont équipés aujourd'hui de box ADSL. On peut imaginer des offres qui intègrent la sécurité dans ces boîtes pour des PME qui n'ont pas besoin de comprendre comment cela marche, ni de devenir expertes en cybersécurité pour être protégées de manière efficace. À l'inverse, si elles doivent paramétrer les pare-feu, c'est très compliqué et c'est probablement voué à l'échec. Il reste beaucoup de travail à faire, pour les grands groupes aussi.

Sur la question du financement, je n'ai pas d'avis. Ce n'est pas vraiment de ma compétence. Il me semble normal que la cybersécurité entre dans le budget de fonctionnement des entités. Ponctuellement, on pourrait les aider ou les inciter. Cette piste mérite d'être explorée.

M. Philippe Vitel. Les collectivités locales ont-elles un rôle à jouer ?

M. Guillaume Poupard. Probablement oui, mais je ne suis pas un expert. Nous connaissons l'exemple de la région des Hauts-de-France qui vient de lancer un fonds permettant aux entreprises de mener des audits de sécurité. Cela me paraît une démarche très élégante : on ne prend pas en charge la sécurité de l'entreprise, on l'aide à prendre conscience du travail à accomplir. Nous disposons d'un programme de qualification de prestataires d'audit, comme pour le *cloud computing*. Quelqu'un qui veut faire appel à un prestataire compétent et de confiance pour établir un diagnostic de la sécurité de son réseau informatique peut consulter la liste de prestataires qui figure sur notre site internet et qui lui garantit que ces entreprises fourniront un service de qualité et de confiance.

La formation est un des cinq axes de la stratégie nationale. Elle est indispensable car la France manque d'experts. L'ANSSI est accusée de tous les recruter – ce n'est pas exact. Le nombre d'experts est insuffisant au regard des besoins, dans le public et dans le privé.

La question de la formation se pose pour toutes les personnes qui vont travailler dans les métiers du numérique. Je vois beaucoup de bac + 5, ceux qu'on appelait les informaticiens, qui n'ont pas eu une minute de formation sur la sécurité au cours de leur cursus. Si ces personnes ne sont pas rattrapées ou ne s'y intéressent pas par elles-mêmes,

pendant toute leur vie, elles vont coder des informations qui ne seront pas sécurisées. Nous travaillons beaucoup avec les formations supérieures et avec les écoles d'ingénieurs. Là encore, nous avons mis en place un programme de labellisation, appelé SecNumedu qui a été lancé au Forum international de la cybersécurité (FIC) la semaine dernière. Nous avons déjà labellisé 26 formations supérieures, plutôt pour des experts, pour lesquelles nous garantissons qu'elles respectent des critères et vont former de bons ingénieurs ou de bons experts dans le domaine cyber. En dépit de notre retard, on trouve de très bons experts en France. Nous souffrons d'un problème non pas qualitatif mais quantitatif en matière de formation.

Quant aux moyens, l'ANSSI en a. Il faudra veiller dans les années à venir, dès 2018, à ce qu'ils demeurent. L'ANSSI n'a pas été oubliée, loin de là. Ses effectifs sont passés d'une centaine à sa création en 2009 à 500 personnes aujourd'hui. Je fais probablement partie des directeurs heureux de ce point de vue-là.

Nous avons été fortement soutenus. Nous aurons à maintenir une croissance, peut-être pas aussi rapide, pour être capable d'absorber les nouvelles missions qui nous sont confiées et pour bien faire notre travail.

S'agissant de notre travail dans les régions, nous avons fait notre autocritique. L'ANSSI était très parisienne, très centralisée – c'est le propre d'une direction centrale. Il m'arrivait de taquiner mes collègues en leur demandant : quand allez-vous passer le périphérique ? Nous avons fait le choix d'aller vers les régions car, de manière surprenante, les problématiques ne sont pas les mêmes d'une région à l'autre. Les messages qui nous semblent audibles à Paris ne le sont pas en région car, dans certaines d'entre elles, nous n'avons pas de relais. Il y a des cas particuliers comme la Bretagne, dans laquelle le ministère de la Défense est très présent, ce qui compense très largement cette absence. Dans certaines régions, les questions de cybersécurité n'étaient portées par personne. Nous avons mis en place un référent territorial par région – treize personnes, c'est à la fois peu et beaucoup à notre échelle. Ce référent a pour mission, non pas de s'occuper de la sécurité informatique de la préfecture, mais de diffuser nos messages en région et d'être un capteur pour nous faire remonter les difficultés. Cette approche régionale est très récente – elle a été mise en place en 2016. Les premiers retours sont très positifs. Nous allons probablement continuer dans ce sens. Il ne s'agit pas de devenir une administration décentralisée avec des dizaines de personnes dans chaque région, mais de renforcer notre présence pour bien couvrir l'ensemble du territoire et pour avoir un accès direct aux PME.

Concernant l'ENISA, nous suivons de près les travaux de cette agence. Au niveau européen, nous défendons l'idée d'une Europe qui traite de cyberdéfense tout en préservant la souveraineté nationale. Nous devons constamment concilier ces deux impératifs. L'ENISA n'est pas l'équivalent de l'ANSSI : elle est dépourvue de capacité opérationnelle ou de traitement d'alerte ; elle travaille sur la prévention en amont, l'identification des problématiques et le *capacity building*, à savoir le soutien aux États membres qui souhaitent – c'est même une obligation désormais avec la directive NIS – développer une capacité de cyberdéfense.

Le conseil d'administration de l'ENISA est présidé par un Français, Jean-Baptiste Demaison, qui est un agent de l'ANSSI. Nous souhaitons encourager l'ENISA car l'homogénéisation au niveau européen nous semble essentielle, par solidarité européenne mais aussi parce que nous ne voulons pas de pays à la traîne qui deviendraient des foyers

d’infection. C’est là que les attaquants vont agir. Nous avons besoin d’une cohérence au niveau européen. La directive NIS va nous y aider, l’ENISA aussi.

Reste la question de la sécurité des institutions européennes, qui n’est pas traitée par les États membres. Nous travaillons avec les institutions, notamment sur le développement de ce que l’on appelle le CERT-EU – *Computer Emergency Response Team* –, un centre opérationnel consacré à leur sécurité. Il reste beaucoup à faire car les institutions sont souvent mal pourvues en termes de sécurité informatique – certains s’y retrouvant probablement... Nous suivons cela de très près en veillant à ce que cela n’empiète pas sur des questions de souveraineté nationale. C’est cet équilibre que nous devons trouver.

S’agissant du dispositif ACYMA, aujourd’hui, la victime d’une attaque informatique peut porter plainte – nous l’encourageons à le faire –, mais c’est encore très compliqué et cela n’apporte pas de solution pratique. Ce problème nous préoccupait depuis un moment. Je ne souhaite pas que l’ANSSI fasse le grand écart entre le CAC40 et les citoyens ; elle risque de s’y perdre. D’où l’idée d’un dispositif spécifique qui prend la forme d’un groupement d’intérêt public (GIP), dont les statuts ont été validés par Matignon la semaine dernière. Ce GIP doit associer les administrations – l’ANSSI, le ministère de l’Intérieur, le ministère de la Justice, le secrétariat d’État au numérique, Bercy – et des opérateurs privés qui ont intérêt à l’élévation du niveau de sécurité de nos concitoyens. Nous appelons ceux qui fournissent des services ou des produits ainsi que les associations de consommateurs à participer au GIP pour diffuser des messages de prévention. Nous avons besoin de faire de la sécurité numérique une grande cause nationale. Il faut porter des messages auprès de nos concitoyens, nous ne l’avons pas encore fait. Il faut aussi apporter des solutions pratiques en cas d’attaque afin que chacun puisse trouver une aide concrète. Les citoyens ne vont pas la trouver auprès des prestataires qualifiés par l’ANSSI, encore moins auprès de l’ANSSI elle-même qui n’en a pas les moyens, mais auprès des prestataires informatiques – la petite boutique du coin qui vend du matériel, qui est capable de réinstaller un disque dur. Ce sont eux qui peuvent apporter des solutions aux clients de petite taille. ACYMA est une plateforme informatique qui permettra aux victimes d’être mises en relation avec des personnes capables de leur apporter une aide concrète.

ACYMA nous permettra aussi de recueillir des chiffres – on parle beaucoup de cybercriminalité mais il n’existe pas d’observatoire de ce phénomène. L’absence de données est un obstacle pour les assurances qui voudraient développer des polices dans le domaine de la cybersécurité – ce que demandent les PME notamment. Aujourd’hui, les assureurs sont incapables de faire tourner leur modèle et de quantifier le risque. Nous travaillons avec eux sur ACYMA afin de pouvoir demain assurer le risque résiduel, ce qui ne doit pas dissuader de se protéger.

À la question « sommes-nous assez protégés ? », la réponse est non. Nous allons être confrontés encore longtemps à des catastrophes. Notre ambition est de les éviter au maximum. C’est la raison pour laquelle nous sommes très volontaristes, nous travaillons sur la réglementation, nous secouons, parfois un peu fort, des victimes potentielles pour leur dire qu’elles sont complètement inconscientes, toujours dans leur intérêt, et avec les opérateurs d’importance vitale, dans l’intérêt de la Nation. L’attaque conservera probablement l’avantage encore longtemps. Il ne faut pas pour autant être fataliste mais bien mettre en œuvre des solutions efficaces, même si elles sont un peu coûteuses.

Concernant le vote électronique et les élections, il y a plusieurs types de risques. Si je devais résumer, un premier risque pèse sur les entités institutionnelles – les réseaux du ministère de l'Intérieur mobilisés notamment pour collecter les résultats et faire les additions. Nous travaillons avec le ministère de l'Intérieur pour sécuriser les réseaux ; c'est un peu notre domaine de confort puisque nous avons l'habitude de travailler avec les administrations, nous connaissons les recettes. Cela se passe bien. Nous travaillons également avec le ministère des Affaires étrangères sur la question plus complexe du vote des Français de l'étranger. Le choix a été fait de ne pas autoriser le vote électronique pour l'élection présidentielle mais seulement pour les élections législatives – en cas d'invalidation, les conséquences ne sont probablement pas les mêmes. Je suis personnellement un peu inquiet – je ne suis pas le seul, les experts partagent mon inquiétude – sur la sécurisation de ce type de vote. À la fin, le votant est devant son ordinateur et la sécurité de l'ordinateur n'est pas maîtrisée, on ne sait pas ce qu'il s'y passe. Pour des attaquants de très haut niveau, les manières de faire dysfonctionner le processus sont multiples. Il ne s'agit pas nécessairement de modifier les chiffres – c'est certainement ce qu'il y a de plus compliqué –, mais de bloquer les systèmes, de les rendre inopérants. Ces techniques sont probablement à la portée des très grands acteurs. On a vu qu'ils s'intéressaient aux élections américaines. On ne peut totalement exclure qu'ils n'aillent pas également s'intéresser aux élections françaises ou allemandes.

Autre sujet, les machines à voter. Ce sont de vieux systèmes, souvent obsolètes mais qui peuvent être connectés. C'est un domaine que nous connaissons mal car nous n'avons pas été amenés à les homologuer. Je ne veux pas porter un jugement sur des produits que nous n'avons pas examinés. Si je peux me permettre une appréciation personnelle, on se passerait bien de ces machines qui posent un vrai problème.

Mme la présidente Patricia Adam. Mais si elles ne sont pas connectées ?

M. Guillaume Poupard. Ces machines sont forcément connectées à un moment, ne serait-ce que pour les paramétrer et ensuite pour récupérer l'information. Avec un peu de chance, ce n'est pas plus risqué qu'une manipulation dans une urne. Pour être franc, nous ne sommes pas totalement à l'aise avec ces machines, qui sont anecdotiques sans l'être. Environ un million de votants les utilisent. Elles font toutefois l'objet d'un moratoire depuis 2007, qui interdit de mettre en service de nouvelles machines, preuve que des doutes existaient déjà à l'époque sur la sécurité.

Les autres systèmes qui peuvent être ciblés – c'est le retour d'expérience de la campagne américaine –, ce sont les systèmes d'information des partis politiques eux-mêmes. Pour nous, c'est beaucoup plus complexe à traiter : il est hors de question que l'ANSSI pénètre directement dans ces systèmes. Nous avons donc organisé un séminaire pour sensibiliser les partis – ils l'étaient déjà – à la nécessité de se protéger. Nous connaissons les solutions, ce sont celles que nous préconisons pour les PME ; un parti politique, du point de vue informatique, est une grosse PME. Nous ne sommes pas sereins. Le scénario consistant à aller voler des courriels pour faire de la désinformation ensuite ou porter atteinte à l'image pose problème, non pas que tout le monde détienne des choses délictueuses dans ses boîtes aux lettres mais le contenu de ces courriers relève de la correspondance privée ; il n'a pas vocation à se retrouver sur internet. S'y ajoute le risque ultime de modification : des faux peuvent se glisser dans ces correspondances. Dans ce cas, la falsification est très difficile à prouver, avec des conséquences que l'on ne sait pas quantifier aujourd'hui.

Dernier risque, ce sont les réseaux sociaux. Sans parler de cyberattaque, on observe des manipulations – la campagne américaine en a connues. Des internautes font remonter sur Youtube, de manière anormale, des vidéos complotistes ou extrémistes notamment qui n'ont rien à faire là. Certains acteurs – on ne sait pas où ils sont – jouent avec les règles, à la limite de la légalité, pour essayer de manipuler l'information en utilisant les propriétés des réseaux sociaux.

Il est vrai que, depuis la loi Lemaire, les personnes de bonne foi peuvent nous signaler des failles informatiques. Nous recevions déjà des signalements, et, de mémoire, nous n'avons jamais appliqué l'article 40 du code de procédure pénale et avisé le procureur. Toute forme d'intrusion informatique est délictueuse. Mais le débat est de savoir où est l'intrusion informatique. Ce débat n'est pas simple.

L'adoption de cet article a rassuré un certain nombre de personnes qui nous signalent des choses, ce qu'elles ne faisaient pas par le passé, parfois des choses importantes. C'est un capteur de plus que j'accepte avec plaisir.

À propos des risques pouvant toucher l'industrie, il existe des systèmes de contrôle de processus dont l'interface de commande est directement accessible depuis Internet. L'exemple le plus glauque que je connaisse est celui d'un crématorium : des internautes, sans capacité de cyberattaque, pouvaient modifier les paramètres du crématorium. C'est incroyable, le système était à la portée de n'importe quel plaisantin. Les exemples de ce type sont assez nombreux. C'est plutôt ce genre de signalement que nous recevons. L'article de loi a rassuré, on ne voit pas aujourd'hui d'effets pervers dans cette démarche. Au contraire, il contribue plutôt à responsabiliser des citoyens numériques, ce qui est probablement une très bonne chose.

Concernant la coopération européenne, elle constitue un de nos axes de travail importants pour 2017 et 2018 : notre objectif est de trouver une dynamique au niveau européen et de ne pas rester uniquement au niveau franco-français. La directive NIS et sa transposition seront une étape importante. Nous aurons besoin d'un « véhicule » législatif – peut-être une loi autonome, pour ne pas devoir attendre – pour transposer cette directive et étendre la réglementation à d'autres acteurs que les opérateurs d'importance vitale. Vous aurez évidemment un rôle fondamental à jouer.

Cette directive encourage la coopération européenne. Celle-ci est aujourd'hui d'une double nature : d'une part, la coopération sur les principes, les règles de sécurité, voire sur des questions industrielles ; elle se développe, c'est très positif ; d'autre part, des coopérations extrêmement sensibles dans lesquelles nous traitons de victimes et d'attaquants, des coopérations opérationnelles pour lesquelles nous resterons encore longtemps dans un cadre bilatéral parce que les éléments manipulés sont extrêmement sensibles ; les sources d'information, ce sont soit les victimes elles-mêmes que l'on veut protéger, soit les services de renseignement avec toute la précaution que nécessite la manipulation de ce genre d'informations. Nous pouvons le faire avec les pays avec lesquels la confiance est établie. Nous ne sommes pas prêts à le faire à vingt-huit.

Mme la présidente Patricia Adam. Monsieur le directeur général, je vous remercie pour toutes les informations que vous nous avez apportées.

La séance est levée à dix-huit heures.

*

* *

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. Jean-Jacques Candelier, M. Jean-David Ciot, M. David Comet, Mme Geneviève Gosselin-Fleury, M. Alain Moyne-Bressand, M. Eduardo Rihan Cypel, M. Jean-Michel Villaumé, M. Philippe Vitel

Excusés. - Mme Danielle Auroi, M. Claude Bartolone, M. Philippe Briand, M. Guy Delcourt, Mme Carole Delga, M. Nicolas Dhuicq, Mme Geneviève Fioraso, M. Serge Grouard, Mme Edith Gueugneau, M. Francis Hillmeyer, M. Éric Jalton, M. Jean-Yves Le Déaut, M. Frédéric Lefebvre, M. Christophe Léonard, M. Maurice Leroy, Mme Lucette Lousteau, M. Alain Marty, Mme Marie Récalde, M. François de Rugy, M. Manuel Valls

Assistaient également à la réunion. - M. Jean-Claude Bouchet, Mme Virginie Duby-Muller