ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire 2

Jeudi
8 mars 2018
Séance de 11 heures

Compte rendu n° 53

SESSION ORDINAIRE DE **2017-2018**

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

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures.

M. le président Jean-Jacques Bridey. Mes chers collègues, nous sommes réunis pour entendre, pour la première fois, M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), sur le projet de loi de programmation militaire. Je lui souhaite la bienvenue.

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information. J'ouvrirai mon propos par une mise en perspective des questions de cybersécurité qui intéressent l'ANSSI à temps plein afin d'exposer les menaces que nous devons combattre, ainsi que les choix d'organisation faits par la France depuis quelques années, qui diffèrent de manière assez significative de ce que font nos grands alliés.

J'en viendrai ensuite à l'article 19 de la loi de programmation militaire (LPM), qui va nous permettre, je l'espère, de compléter notre arsenal afin de faire face à ces nouvelles menaces.

Notre sujet est la cybersécurité, c'est-à-dire tout ce qui a trait à la sécurité des systèmes numériques. Même s'il n'y a pas de petites victimes, l'idée est que nous regardons les choses par le haut car le rôle de l'ANSSI est de traiter tout ce qui peut toucher aux questions de sécurité nationale et d'intérêts de la Nation.

Le domaine du numérique peut sembler très éthéré, mais les menaces sont malheureusement très concrètes. Celles qui sont liées à la criminalité ne nous intéressent pas au premier chef même si elles peuvent être liées à nos préoccupations. De fait, l'attaque informatique est un véritable paradis pour les mafieux, les criminels qui veulent pouvoir gagner beaucoup d'argent, escroquer beaucoup de gens, et toucher beaucoup de victimes sans, la plupart du temps, prendre le moindre risque.

Plus grave : nous sommes confrontés depuis maintenant plus de dix ans à des campagnes d'espionnage absolument catastrophiques. La grande difficulté tient au fait que l'attaquant fait tout pour rester discret. En outre, les victimes d'espionnage n'ont pas envie d'en parler, ce que je comprends très bien, et ceux qui les aident, c'est-à-dire très souvent l'ANSSI, protègent leur identité et gardent le secret afin de ne pas ajouter du malheur au malheur.

L'ANSSI traite chaque année une vingtaine de cas d'espionnage grave, ce qui signifie que ce sont des intérêts liés à la sécurité et à la défense nationale qui sont touchés. Cela peut se produire au sein d'un ministère ou, plus souvent, au sein d'entités privées, d'industries : historiquement, les industries d'armement ont été très ciblées par des campagnes d'espionnage et des informations ont ainsi été perdues – pas pour tout le monde ! –, ce qui n'aurait pas dû se produire.

Ce n'est pas parce qu'on n'en parle pas dans les médias que l'espionnage n'existe pas. On en parle parfois lorsque cela devient concret, par exemple la semaine dernière, lorsque, en Allemagne, des attaquants, probablement russes mais nous n'en avons pas la preuve formelle, s'en seraient pris au ministère de la Défense et au ministère des Affaires étrangères.

Cela ne nous surprend pas outre mesure puisque nous détectons ces attaquants alors qu'ils sont en train de chercher à entrer au sein des mêmes ministères en France ainsi que dans probablement tous les pays occidentaux. L'espionnage est donc une véritable menace, mais il n'est pas la pire, si j'établis une gradation dans l'horreur. Le risque le plus important que traite l'ANSSI et, plus généralement, les services de l'État, c'est celui de sabotage, de conflits quasi armés appelés à se développer dans le futur, parce que le numérique constitue le substrat. C'est dans le cyberespace, pour reprendre un terme de journaliste, que se déroulera une bonne partie de ces affrontements.

Le risque n'est ainsi plus uniquement le vol d'informations, qui peut sembler assez éthéré, mais bien l'atteinte physique grave portée à des systèmes, voire leur destruction. Cela peut concerner tout ce qui est industriel, tous les opérateurs dits « d'importance vitale » (OIV) : grands acteurs de l'énergie, des transports, des télécommunications, de l'armement, de l'industrie lourde et d'autres secteurs, tout aussi sensibles pour le fonctionnement de la Nation.

J'insiste sur le fait qu'il ne s'agit pas que d'espionnage, mais bien de destruction. Par les moyens numériques, donc en attaquant depuis le bout du monde, l'agresseur qui prend par exemple le contrôle d'une raffinerie est tout à fait capable de produire des catastrophes, notamment la destruction de systèmes par le biais de l'informatique. De même, dans le domaine du transport, on peut tout à fait imaginer – je ne prétends pas que c'est réalisable, mais cette éventualité doit être prise en compte – le scénario d'un attaquant se rendant maître du système de contrôle de trains ou d'avions, provoquant par là de véritables catastrophes.

Sans chercher à dramatiser, il faut constamment garder à l'esprit que c'est à cela que l'on doit faire face et c'est précisément pour ce faire, que la France a choisi de s'organiser. En la matière, le Livre blanc sur la défense et la sécurité nationale a été une sorte de déclencheur en 2008, soit l'année qui a suivi une attaque majeure contre l'Estonie où, pendant plusieurs semaines – on l'oublie, car le temps passe vite – les transports, le système de santé et le système bancaire ont été paralysés. Les Estoniens ayant eu le malheur non pas d'enlever mais simplement de déplacer la statue érigée à la gloire du soldat russe , cela a provoqué la colère de personnes que le Kremlin avait à l'époque qualifiées de patriotes russes, qui ont mené des attaques informatiques majeures. Or, l'Estonie est le pays le plus numérisé au monde, ce qui constitue une force, mais aussi peut aussi être une sorte de talon d'Achille dès lors que la sécurité numérique associée à ce développement n'est pas assurée.

Le livre blanc de 2008 présente deux éléments essentiels pour la cybersécurité. Le premier, qui ne concerne pas l'ANSSI, est le développement d'une capacité informatique offensive, qui est ainsi assumée. Le second élément a précisément été la création de l'ANSSI, autorité nationale chargée des questions de cybersécurité et uniquement consacrée à la défense, à la protection et à l'aide aux victimes, ainsi qu'à la détection des attaques, mais qui ne fait pas elle-même de renseignement ni d'attaque.

Ce qui peut vous paraître une évidence ne l'est en fait pas puisque nos grands alliés anglo-saxons font exactement l'inverse en confiant la cybersécurité, au sens auquel je l'entends à l'ANSSI, aux services de renseignement technique. Ainsi, mon homologue américain est la *National Security Agency* (NSA), et mon homologue britannique, le *Government Communications Headquarters* (GCHQ).

Ce choix d'un modèle totalement différent regroupant l'attaque et la défense au même endroit, afin de créer une forme de synergie, est toutefois à l'origine de nombre de problèmes tenant à la complexité de missions qui entrent parfois en contradiction. C'est un peu comme si, en France, on avait confié le travail de l'ANSSI à la Direction technique de la direction générale de la sécurité extérieure (DGSE), ce qui présenterait des avantages, mais aussi beaucoup d'inconvénients, notamment au regard de la confiance vis-à-vis des victimes que nous aidons régulièrement.

Quelques chiffres. L'ANSSI emploie aujourd'hui 550, contre 80 en 2009, lors de sa création. C'est une croissance colossale. Elle est composée à 95 % d'experts techniques de très haut niveau, dont 80 % sont des contractuels civils : tel est le profil d'un service du Premier ministre quelque peu atypique.

Nous développons de nombreuses méthodes de prévention, nous faisons du conseil et, grâce aux dispositions de la précédente LPM, nous sommes en mesure d'imposer la cybersécurité aux opérateurs d'importance vitale. Par ailleurs, la transposition de la directive européenne NIS (*Network and Information Security*), qui reprend cette idée, nous permet « d'imposer » – j'emploie des guillemets parce que tout cela est très coopératif – des mesures de cybersécurité à beaucoup plus d'acteurs qu'auparavant, notamment privés.

Notre première mission porte donc sur la prévention, le conseil, la formation et la réglementation au sens large.

Notre deuxième mission c'est la détection, mais il n'est pas possible de construire des systèmes parfaitement sécurisés, même si c'est ce vers quoi nous tendons dans des cas exceptionnels comme la dissuasion nucléaire, pour laquelle aucun risque n'est concevable. Mais, dans la plupart des cas, il est quasiment impossible de garantir une sécurité à 100 % ; ceux qui affirment le contraire sont des menteurs.

Nous faisons de la sécurité, de la protection et nous concevons des systèmes de bonne tenue. Nous complétons le risque résiduel par la détection des attaques qui ont tenté de passer en dépit des protections prises.

L'ANSSI développe, opère, déploie des systèmes de détection d'attaque – des « sondes » dans notre jargon technique –, au profit de l'ensemble des ministères et, très bientôt, de l'Assemblée nationale. Il a en effet été décidé, et je salue cette résolution importante et courageuse, de passer par le système de détection de l'ANSSI pour vous protéger et être capable de détecter au plus tôt des attaquants qui chercheraient à prendre le contrôle de vos ordinateurs, de vos systèmes d'information, qui voudraient connaître vos courriels et vos informations numériques.

Cela ne relève nullement de la fiction : pas plus tard que l'an dernier, nous avons arrêté des attaques qui visaient l'Assemblée nationale. On se souvient, par ailleurs, de l'attaque menée contre le *Bundestag* en 2015 par le même attaquant que celui qui s'en était pris à TV5, qui s'en est pris ensuite au Comité national démocrate lors de la campagne des élections américaines. Dans le jargon, nous appelons cet attaquant APT28 que les sources ouvertes – que je me borne à citer – identifient comme un important service russe de renseignement. Nous avons donc conscience qu'une menace pèse sur les parlementaires et, pour continuer à vous faire peur, vos collègues britanniques ont aussi été attaqués l'an dernier

de manière assez massive ; il est donc important d'être capable de détecter ces attaques pour vous protéger.

Notre troisième mission, la réaction, réside dans l'aide apportée aux victimes : avec des équipes de pointe, nous sommes capables – que ce manque de modestie me soit pardonné – de secourir les victimes les plus sensibles en cas d'attaque avérée, ce qui signifie les protéger très rapidement, dans les premières heures, pour ensuite les aider à reconstruire, ce qui est primordial. Nous nous livrons par ailleurs, au profit des autorités, a un travail de développement et d'opérations portant sur les systèmes de communication sécurisés : tous les systèmes interministériels traitant d'informations classifées, qu'il s'agisse des réseaux informatiques, des téléphones ou des éléments visuels, sont développés et opérés par l'ANSSI.

Il faut savoir rester très modeste dans le domaine de la cybersécurité : nous ne faisons pas de la sécurité absolue, nous courrons plutôt après les attaquants, qui sont très agiles et disposent de moyens considérables. Aujourd'hui – et cela m'amène à parler de l'article 19 du projet de LPM – nous souffrons probablement d'une certaine faiblesse dans la détection d'attaques, mais nous savons le faire pour la sphère étatique et nous savons imposer l'installation de systèmes de détection aux opérateurs privés les plus critiques et d'importance vitale.

Nous qualifions des offres privées de détection : lorsque les prestataires de détection d'incidents de sécurité comme Thales, Airbus ou d'autres développent des systèmes de détection, ils sont évalués et qualifiés par l'ANSSI au nom du Premier ministre. Les attaquants passent par les réseaux informatiques, ils compromettent des ordinateurs, rebondissent de serveurs en serveur sans être repérés parce qu'il n'existe pas de mécanisme de détection. Or, la détection est absolument essentielle : la plupart du temps on ne sait même pas que l'on est attaqué ou on le constate trop tard, à cause des dégâts, lorsqu'il s'agit de destruction ou de sabotage, comme dans le cas de TV5.

Le texte qui vous est proposé présente deux évolutions majeures bien distinctes.

La première consiste à instaurer un système de détection globale à grosses mailles en recourant à des acteurs qui ne sont pas utilisés alors qu'ils sont essentiels dans ce monde numérique : les opérateurs de communications électroniques. Ces opérateurs transportent, malgré eux, les attaques depuis les agresseurs vers les victimes ! En effet, les attaques circulent, depuis les attaquants vers les victimes, à l'intérieur du flux de données numériques, en passant par un nombre considérable d'intermédiaires.

Aujourd'hui, les opérateurs français ne font pas de détection d'attaques : l'idée de cette première proposition est de permettre – obliger n'aurait pas de sens – ces opérateurs, sur la base d'éléments dont ils disposent ou d'éléments techniques que l'ANSSI pourrait leur fournir, à détecter des attaques informatiques. C'est dans ce contexte que notre modèle, qui sépare clairement l'attaque et la défense me semble très pertinent pour chercher simplement à découvrir s'il y a quelque chose de malveillant.

Il est difficile de donner une image représentative de notre activité de détection des attaques informatiques, car il s'agit d'un métier très technique et très particulier, mais on pourrait prendre l'exemple des scanners des aéroports : si vous avez un livre dans votre

bagage, la personne derrière l'écran ne le lit pas et ignore même son titre. En revanche, s'il y a des explosifs ou une arme, le système fait apparaître en rouge une forme suspecte.

L'objet de cette analogie, que nous avions choisie lors de la présentation devant le Conseil d'État, est d'expliquer ce que recouvrent cette notion de détection et celle de marqueur technique – la forme du pistolet dans l'exemple du scanner. En fait ce que nous voulons faire c'est en quelque sorte scanner les bagages, mais en étant beaucoup moins intrusifs.

Prenons un autre exemple : si l'on veut savoir, parmi les voitures qui passent, quelles sont celles qui polluent, on ne cherche pas pour autant à savoir à qui appartient le véhicule, on ne lit même pas sa plaque minéralogique, mais on essaie de détecter des événements anormaux, de manière à pouvoir déclencher une vérification – ce que nous appelons une qualification des attaques.

Il s'agit donc de permettre aux opérateurs de faire de telles détections, de permettre à l'ANSSI de donner aux opérateurs des éléments techniques afin de savoir repérer certains attaquants en commençant par les plus actifs, ceux qui nous inquiètent le plus en ce moment. Une partie du travail de l'Agence consiste à établir des marqueurs permettant de détecter des attaquants, qu'il s'agisse d'adresses IP ou internet suspectes, de noms de sites web connus pour être piégés… Bref, il existe de nombreux types de marqueurs différents qu'il serait vain de vouloir les énumérer dans un texte de loi.

Lorsque l'opérateur détecte quelque chose, il faut qu'il puisse nous indiquer vers quelle cible le marqueur que nous lui avons donné est positif, ce qui pourrait indiquer qu'une attaque est tentée. Dès lors, deux possibilités se présentent.

Si l'attaqué est une administration, un opérateur d'importance vitale, cela entre dans le champ d'action de l'ANSSI qui peut demander des éléments complémentaires et aller aider la victime le plus vite possible.

Si les victimes ne relèvent pas du champ d'action de l'ANSSI, qui n'a alors pas les moyens de traiter l'attaque de manière personnalisée, la loi prévoit que l'on puisse demander à l'opérateur de communications électroniques de prévenir les victimes, au moins pour qu'elles sachent qu'elles sont attaquées, ce qui n'est pas évident car, j'insiste sur ce point, cela est très peu visible.

L'autre partie du texte traite un champ totalement différent : nous sommes régulièrement alertés, presque toujours par des partenaires étrangers qui nous signalent, à tel endroit, derrière telle adresse IP d'un ordinateur donné, qu'un agresseur a pris pied, s'est installé et se sert de cette machine pour conduire des attaques.

Comment nos interlocuteurs obtiennent-ils ces informations ? Il arrive que je préfère ne pas savoir parce qu'il s'agit parfois de très grands services de renseignements. Le plus souvent, ce sont des partenaires étrangers qui sont en train de surveiller un serveur qui a été compromis par un attaquant, et qui est en train d'attaquer une autre machine ; c'est ainsi qu'une espèce de réseau se crée. Dès lors, François Deruty, chef du centre opérationnel de l'ANSSI, et son équipe n'ont qu'une envie : aller voir sur cette machine s'il y a réellement un attaquant, et, le cas échéant, ce qu'il est en train de faire.

Si ces machines se trouvent chez des particuliers ou dans des entreprises qui les possèdent, nous allons leur expliquer pourquoi nous souhaiterions y avoir accès. Certains cas sont très intéressants, parfois atypiques : on peut tomber sur des PME, des maisons de retraite, des restaurants, ou des administrations – ce qui nous facilite les choses.

Nous ne débranchons surtout pas l'ordinateur concerné, car nous avons la chance d'être devant une machine sur laquelle l'attaquant est actif et ne sait pas qu'il a été repéré ; nous l'observons « au microscope » afin de voir ce qu'il est en train de faire, qui il est en train d'attaquer, etc.

L'autre cas, en passe de devenir majoritaire, est celui dans lequel ces machines se trouvent chez des gens qui louent des machines, des hébergeurs comme OVH, leader français, mais il en existe beaucoup d'autres. Si nous disons à OVH que nous voulons vérifier ce qui se passe sur telle machine, on nous répond que l'on aimerait bien nous aider, mais que nous n'en avons pas le droit, ce qui est vrai. C'est pourquoi la prochaine LPM nous permettra de caractériser une menace potentielle, sur la base d'une alerte ou d'un renseignement, de manière à nous assurer que c'est bien telle machine qui est en cause.

Bien entendu, nous pourrions demander la permission au détenteur de la machine, à celui qui l'a louée de manière légitime, mais nous ne voulons pas le faire. En effet, dans le meilleur des cas nous tomberons sur une victime que tout cela dépasse complètement : la plupart du temps, ces serveurs sont loués par des particuliers, par des gens que l'on n'a pas envie de mêler à des affaires aussi compliquées. Surtout, le plus souvent, celui qui loue la machine est l'agresseur lui-même, par le biais de systèmes démarqués et de montages comme savent très bien le faire certains services. Or, la dernière personne que l'on a envie de prévenir d'un doute que nous nourrissons pour une machine, c'est évidemment l'attaquant lui-même, car il risque de disparaître instantanément : c'est notre quotidien.

Ce dont nous avons absolument besoin pour progresser dans le domaine de la détection et de la compréhension de ces menaces, c'est d'être capables d'aller voir ce qui se passe sur une machine utilisée par un attaquant.

Voilà donc pour ces deux thématiques très différentes, même si elles sont présentes au sein du même article : d'une part une détection au moyen d'un filet à grosses mailles, mais qui ne signifie pas interception, car les finalités sont totalement différentes, et d'autre part une vision beaucoup plus microscopique et très localisée.

La rédaction de ce texte, largement complétée par le Conseil d'État, vise à poser les garde-fous nécessaires pour éviter que ce dispositif puisse être dévoyé ; un contrôle exercé par l'Autorité de régulation des communications électroniques et des postes (ARCEP) est d'ailleurs prévu à cet effet.

Ces dispositions figurent à l'article 20 du projet de loi, qui habilite le Gouvernement à déterminer par ordonnance les modalités du contrôle des activités de l'ANSSI prévu par l'article 19 ; il pourrait être pertinent de proposer un amendement afin que le contenu de cette ordonnance soit gravé dans le marbre de la loi. L'idée est que l'ARCEP puisse être en mesure d'exercer ce contrôle, car elle est la seule à pouvoir vérifier qu'à aucun moment il n'y a d'accès ou d'exploitation de données qui ne sont pas concernées par le traitement des cyberattaques qui nous intéresse.

M. le président. Merci, Monsieur le directeur général, pour cet exposé très clair et très précis, qui a répondu par avance aux questions que certains voulaient poser.

M. Philippe Michel-Kleisbauer. La Revue stratégique de cyberdéfense mentionne les quatre coopérations mais, seule la coopération au sein de l'Union européenne est vraiment évoquée. Conduisons-nous de telles actions avec des pays non-membres de l'Union, ou qui en feront peut-être partie un jour, comme l'Ukraine ?

Nous savons que les Russes, en recourant à des moyens assez simples, ont tenté avec succès de créer une dissonance disruptive chez les soldats ukrainiens. Notre coopération s'étend-elle jusqu'à ces frontières où nous avons beaucoup à apprendre ?

M. Fabien Gouttefarde. L'article 19 de la LPM donne à l'ANSSI la capacité de poser des capteurs techniques, comme c'est le cas des opérateurs. Selon quels critères l'ANSSI prend-elle l'initiative de le faire ou de s'en remettre aux opérateurs ?

M. Stéphane Trompille. Vous avez indiqué avoir contraint certains acteurs privés, du secteur bancaire par exemple, à se conformer aux normes. Quelque chose est-il prévu pour les petites entreprises et les petites collectivités afin d'aller au-delà de la seule sensibilisation ? Car ces entités constituent autant de portes ouvertes aux cyberattaques.

M. Thibault Bazin. Les possibilités que vous attribuez aux opérateurs entraînent-elles des responsabilités ? Si un incident advenait, ne risquerait-on pas de voir les divers acteurs se rejeter la responsabilité, dès lors que l'on se situerait dans le registre des possibilités et non des obligations ?

Par ailleurs, une réforme des documents classés secret-défense est en cours, les critères de classement proviennent-ils de vous afin de pouvoir désigner les cibles, notamment au sein des entreprises traitant de sujets classés ? Cette classification vous permet-elle, le cas échéant, de vous tourner vers les opérateurs ?

M. Guillaume Poupard. La coopération est un sujet vaste et complexe. Nous coopérons de façon bilatérale dans les domaines les plus sensibles. Nous coopérons très bien avec deux grands acteurs. Nous sommes très proches de l'Allemagne en termes d'organisation et de manière de penser. La coopération s'exerce dans pratiquement tous les domaines avec ce pays, et notre homologue, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI), qui se trouve au sein du ministère de l'Intérieur, bien que le travail relève de l'interministériel, envie le positionnement de l'ANSSI. L'autre grand partenaire est le Royaume-Uni, avec qui nous pratiquons une coopération opérationnelle de très haut niveau : c'est probablement notre premier partenaire opérationnel.

Pour être très direct, on ne peut pas faire abstraction de l'épisode Snowden, on ne peut pas faire abstraction de tout ce dont on se doutait et dont nous avons la preuve aujourd'hui : les services de renseignement font du renseignement, y compris sur des cibles qui peuvent être françaises, y compris étatiques. La coopération est donc est très fine : toute information que nous donnons ou que nous recevons est pesée de manière extrêmement délicate.

Nous travaillons également avec les Américains, même si cela est plus compliqué à cause d'un problème de taille bien connu.

À l'échelon européen, nous développons un réseau d'agences homologues de l'ANSSI, c'est à cela que la Revue stratégique de cyberdéfense fait allusion. Nous avons besoin d'un réseau à vingt-huit ou à vingt-sept pour échanger beaucoup plus que nous le faisons aujourd'hui, notamment sur le plan opérationnel.

Au-delà, nous avons des partenaires historiques privilégiés. Nous nous entendons très bien avec le Maroc, avec qui nous nous entraînons : ce pays est très sensible à notre manière de faire, notamment dans le domaine du règlement. Nous travaillons beaucoup avec Singapour, qui est une porte d'entrée classiquement plus facile vers l'Asie, et qui connaît également des problématiques qui nous intéressent particulièrement. En France on parle de *Smart Cities* (villes intelligentes), les Singapouriens de *Smart Nation* parce que la ville se confond avec la nation. Nous travaillons beaucoup avec eux à la protection des opérateurs locaux d'importance vitale et des infrastructures critiques.

Nous avons donc toute une galaxie de coopérations bilatérales et multilatérales, et toute une diplomatie – je ne parle pas encore de coopération – se met en place, y compris avec des pays comme la Chine. Nous avons besoin de parler cyber avec eux, mais nous le faisons *via* le Quai d'Orsay – chacun son métier –, notamment avec l'ambassadeur pour le numérique David Martinon. Nous parlerons dorénavant de plus en plus avec des partenaires un peu plus éloignés d'un point de vue idéologique.

Quant aux capteurs des opérateurs, le fait que la question soit traitée en un seul article peut créer un peu de confusion, mais il faut faire la distinction.

D'une part, les opérateurs vont développer leurs capteurs. Et avant même de le faire, ils vont simplement exploiter toutes les informations dont ils disposent déjà : pour gérer leurs réseaux d'opérateurs de communications électroniques, ils ont énormément d'informations. Ils s'interdisent d'y chercher des traces d'attaque, mais ils ont déjà ces informations. Il s'agit vraiment de *big data* et il faudra demain recourir à l'intelligence artificielle pour fouiller dans ces données tant elles sont hétérogènes et nombreuses.

D'autre part, les capteurs de l'ANSSI, objet du II de cet article 19, seront mis au plus près des machines identifiées. Contrairement à ce qu'ont dit certains médias, il est hors de question que l'ANSSI aille placer des capteurs dans les cœurs de réseau des opérateurs. Je n'ai aucune envie de le faire, ce serait très compliqué et très risqué, même en termes de responsabilité. Il est important que les opérateurs restent maîtres de leur cœur de réseau. Ce sont des systèmes d'une très grande complexité et je n'imagine pas des experts, même très bons, y mettre les mains. Je n'ai aucune envie d'être considéré responsable de défauts ou de problèmes qui seraient constatés.

Il s'agit donc de deux réalités très différentes, qui ne se confondent pas, mais qui peuvent se répondre. Si l'opérateur soupçonne ou détecte une attaque, il pourra identifier une adresse IP sur laquelle l'ANSSI ira poser une sonde – mais ce sera en général chez un hébergeur pas chez un opérateur de communications électroniques.

Quant aux acteurs privés, en effet, il y a des acteurs importants, les opérateurs d'importance vitale et, demain, à la suite des évolutions réglementaires, les opérateurs de services essentiels. Nous leur imposons, en quelque sorte, la cybersécurité. Nous leur imposons la coopération, nous leur fixons des règles, dont l'obligation de faire de la détection, nous leur imposons de nous dire quand ils sont attaqués. La France a été le premier pays au

monde à développer une telle approche réglementaire, et nous pouvons en être fiers : ce n'était pas gagné, mais cela a fait tache d'huile. Toute l'Europe retient dorénavant une telle approche et d'autres pays, même les États-Unis, commencent à considérer que la question est trop grave pour que l'on s'en tienne au conseil.

Cette approche réglementaire n'a cependant de sens qu'à l'égard d'acteurs organisés qui disposent de moyens importants. Ce n'est pas pertinent avec des petites et moyennes entreprises (PME), des collectivités locales ou des particuliers. Je n'imagine pas que l'on impose demain la cybersécurité aux PME ; cela n'aurait aucun sens. Il faut aider les PME. Nous ne pouvons demander au patron de PME qui s'occupe de l'informatique de son entreprise lorsqu'il a une heure le dimanche soir de devenir expert en cybersécurité. En revanche, il est impératif que les solutions auxquelles il recourt soient nativement sécurisées. Le *cloud computing* est une source de menaces supplémentaires, mais si une PME ou une collectivité locale opte pour une solution sécurisée afin de se « débarrasser » de l'informatique, qui représente une charge pour elle car ce n'est pas son métier, elle paiera peut-être un peu plus pour un service sécurisé, mais il ne lui restera qu'à appliquer des règles élémentaires : faire attention à ses clés USB, à ses smartphones, etc. Nous en revenons donc à la sensibilisation, et à des comportements à la portée des personnes : ne pas faire n'importe quoi avec ses mots de passe, c'est simple. En revanche, leur demander de comprendre ce qu'est une attaque informatique et de la détecter quand elle arrive, n'a pas de sens. Nous travaillons beaucoup au développement d'offres sécurisées – il reste fort à faire ; nous soutenons le développement de certaines, notamment *via* le programme d'investissements d'avenir, mobilisé au moins à cinq reprises pour cela.

Nous travaillons avec certains industriels importants, qui sont conscients de la nécessité de sécuriser leur écosystème. Les attaquants attaquent où il est facile de le faire. Celui qui ne sait pas attaquer un opérateur d'importance vitale s'en prendra à ses sous-traitants – je ne prétends pas que les attaquants ne savent pas attaquer les opérateurs d'importance vitale, mais le jour où ils ne pourront plus du tout le faire, ils s'en prendront à toute la myriade de ses sous-traitants. Un industriel comme Airbus l'a très bien compris, qui est en train de promouvoir le développement de solutions sécurisées au profit de son écosystème. C'est une excellente démarche ; nous les y encourageons et les y aidons.

Quant à la responsabilité des opérateurs, je vous livre l'historique récent. Il y a un an les box de *Deutsche Telekom* ont été la cible d'une assez grave attaque. Les parlementaires allemands, qui l'ont convoqué, ont interrogé à juste titre le patron de *Deutsche Telekom* : comment était-ce possible, et qu'avait-il fait pour s'en prémunir ? Simplifions à peine : il a répondu qu'il n'avait rien fait car il n'en avait pas le droit. Le Parlement lui en a donc donné le droit, et la loi allemande, dont nous nous sommes inspirés, a un an d'avance sur nous. Elle n'impose pas aux opérateurs de faire de la détection – cela n'aurait pas de sens aujourd'hui – mais elle le leur permet. L'idée est d'exercer ainsi une sorte de pression pour que les opérateurs fassent ce travail de détection et pour que les clients eux-mêmes demandent aux opérateurs de le faire. Ce raisonnement m'a paru particulièrement malin, d'autant que cette démarche utile et habile permet d'éviter certains écueils, qui tiennent par exemple à la neutralité du net.

Évidemment, nous avons parlé de cela aux opérateurs : qu'en était-il de la faisabilité technique et de leur volonté ? Ils sont prudents, car cela coûtera un peu d'argent et fera peser sur eux, de fait, une forme de responsabilité. Ils ont cependant bien compris que le travail

d'un opérateur de communications électroniques ne pouvait plus être simplement de veiller à ce qu'une attaque aille bien de l'attaquant à la cible – je caricature à peine. Ils ont envie de faire plus de sécurité ; certains ont au moins l'intuition du fait que l'opérateur du futur fera de la distribution sécurisée de données. Orange, dont l'activité de cyberdéfense est importante, l'a d'ailleurs clairement dit : à l'avenir, il s'agira en somme de distinguer entre ceux qui distribuent de l'eau potable et ceux qui distribuent de l'eau non potable. Les opérateurs devront fournir de l'eau potable à leurs clients.

M. le président. C'est presque un argument commercial !

M. Guillaume Poupard. Nos intérêts et ceux des opérateurs ne sont pas contradictoires. Ils peuvent y trouver un intérêt éthique et peut-être même, effectivement, un intérêt commercial.

Quant au secret de la défense nationale, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) travaille depuis plusieurs années à une nouvelle version de l'instruction générale interministérielle n° 1300. C'est un bouleversement majeur de l'approche réglementaire de la protection du secret de la défense nationale. Jusqu'à présent, et encore aujourd'hui, on ne protège pas de l'information, on protège des documents – vous voyez à quel point cette approche est obsolète, même s'il existe encore des documents.

Le changement des dénominations est simplement un alignement avec nos partenaires, notamment l'Organisation du traité de l'Atlantique nord (OTAN). Par exemple, le « confidentiel défense » français est l'équivalent du « *NATO secret* ». Ces décalages posent, dans la pratique, des problèmes infinis, que nous allons régler en faisant un « secret » français du même niveau que le « secret » de l'OTAN. Au-delà, le cœur du travail sur cette nouvelle instruction générale interministérielle n° 1300, c'est de protéger l'information, notamment l'information numérique. Nous sommes intervenus aux côtés de nos collègues du SGDSN dans l'élaboration des règles de sécurité qui s'appliqueront aux différents niveaux de classification à la suite de cette nouvelle instruction générale interministérielle n° 1300. C'est une évolution majeure et, sans doute, le sens de l'histoire. De plus en plus, c'est bien de l'information que nous devrons classifier, non, comme aujourd'hui, des supports ou des documents.

Mme Françoise Dumas. Monsieur le directeur général, je vous interrogerai tout d'abord au nom d'Olivier Gaillard, rapporteur spécial des crédits de la mission « Défense » du budget, retenu dans l'hémicycle. Cette loi de programmation militaire témoigne d'une volonté forte d'investir dans la cybersécurité et la cyberdéfense et d'une coopération entre les opérateurs de télécommunications et l'ANSSI, mais disposez-vous d'une estimation des pertes économiques résultant des cyberattaques ?

Quant à moi, je souhaite vous interroger sur la prévention. Comment l'appréhendez-vous techniquement ? Quelles sont les marges de progression dans la sensibilisation des personnels des collectivités territoriales et des grandes entreprises ? Je suis persuadée qu'elles restent importantes, car tout le monde n'a pas encore conscience de notre vulnérabilité. Comment aller plus loin encore ?

M. M'jid El Guerrab. Qu'en est-il, Monsieur le directeur général, de ces crypto-monnaies – bitcoin, ether, litecoin – que nous avons vu émerger et de leur valorisation parfois folle ? Sont-elles susceptibles de déstabiliser nos économies ? Que se cache-t-il

derrière ces échanges ? Et sommes-nous en mesure de les « tracer » pour nous assurer qu'ils ne financent pas le terrorisme et d'autres activités criminelles ?

M. Fabien Lainé. S'agissant de la sécurisation des infrastructures critiques françaises, nous comptons plus de 200 opérateurs d'importance vitale. Félicitons-nous des dispositions prises dans le cadre de la LPM de 2013 : nous étions quand même très en avance. J'imagine que ces OIV ne sont pas tous pareillement vulnérables. Pouvons-nous faire le point ?

Pouvez-vous aussi nous parler de la sonde souveraine Cybels Sensor de Thales ?

M. le président. Jean-François Eliaou est le rapporteur pour avis de la commission des lois sur la LPM.

M. Jean-François Eliaou. Je voudrais vous interroger sur la relation entre l'ANSSI et l'ARCEP. Le commentaire de l'ARCEP sur l'article 20 n'est pas forcément très favorable, quel est votre sentiment ?

Quant à l'article 19, sera-t-il un outil législatif suffisant ou bien n'offre-t-il pas une cible supplémentaire en entraînant une fragilité propice aux attaques ?

M. Guillaume Poupard. À propos des pertes économiques occasionnées par les cyberattaques, des chiffres circulent, qui donnent le vertige, mais je ne suis pas en mesure de les confirmer. On parle, au ministère de l'Intérieur, de « chiffre noir », car, effectivement, nous ne savons pas l'évaluer.

Ce qui est certain, c'est que les risques de perte sont incommensurables. Si, demain, des actes de terrorisme, des actes de guerre détruisent nos opérateurs d'importance vitale, bloquent nos systèmes de transport, nous coupent l'électricité, cela nous coûtera extrêmement cher. Techniquement, ce sont des possibilités qu'il ne faut pas exclure, le phénomène se développe même. De ce point de vue, les cyberattaques subies par l'Ukraine témoignent de l'étendue des dommages que peuvent causer les attaques informatiques. Tout y a déjà été testé. L'électricité a été coupée, les systèmes de transport ont été paralysés. Les attaques sont régulières et « éclaboussent » parfois d'autres victimes. Ainsi, l'activité de Saint-Gobain, qui avait un bout de réseau en Ukraine, a été bloquée pendant quinze jours. Nous les avons beaucoup aidés, cela s'est bien passé, et nous les connaissons maintenant bien, mais, pendant quinze jours, ils ne savaient plus où devait être livré ce qu'ils produisaient et ils ne pouvaient plus prendre de nouvelles commandes. Cela a eu un impact de 240 millions d'euros sur le chiffre d'affaires et de 80 millions – l'équivalent du budget de l'ANSSI – sur le résultat net. C'est là l'effet d'une attaque ayant paralysé quinze jours l'activité d'un opérateur qui n'est même pas d'importance vitale et n'a pas vocation à le devenir ! Malheureusement, les chiffres s'envolent très vite. Régulièrement, on me demande s'il ne suffirait pas d'un fonds, comme celui dédié aux catastrophes naturelles, pour faire face de telles attaques. Ce n'est pas possible, car nous ne sommes pas capables d'en fixer le montant, et, quand bien même nous le doterions d'un milliard, l'exemple de Saint-Gobain montre que les dégâts d'une attaque pourraient très vite atteindre un tel coût. Cela ne veut pas dire que l'approche assurantielle n'a pas de sens. Au contraire, nous y travaillons, en lien étroit, dans le cadre de la Revue stratégique de cyberdéfense, avec les acteurs concernés.

En matière de prévention, entre ce que nous imposons réglementairement et ce que certains font de manière volontaire, cela fonctionne très bien. La marge de progression n'en reste pas moins colossale ; je suis d'accord avec vous.

Le degré de sécurité des différents opérateurs, qu'ils soient publics ou privés, est très hétérogène. Évidemment, le problème présente une dimension technique. Il faut être en mesure d'intégrer de la sécurité dans les systèmes dès leur conception – *by design*, comme disent les industriels. Se posent cependant également des questions de gouvernance. J'en avertis les comités exécutifs des grandes entreprises : la cybersécurité est de leur responsabilité et de celle des conseils d'administration, non de celle d'un responsable de la sécurité des systèmes d'information perdu au fin fond de l'organigramme. La menace est telle et implique des arbitrages d'une importance telle que la question doit être examinée au plus haut niveau. Je tiens exactement le même discours aux administrations et aux ministères.

S'il est très difficile d'évaluer le coût de la cybersécurité, on estime aujourd'hui qu'il représente entre 5 % et 10 % du budget informatique d'une structure, il est donc considérable, puisque les budgets sont considérables. Ce n'en est pas moins accessible, le budget ne s'en trouve pas multiplié par dix. L'idée est que chacun puisse prendre les bons arbitrages en la matière.

Les crypto-monnaies n'entrent qu'à la marge dans notre champ de compétence. Nous en subissons les effets dans nombre d'actes cybercriminels car, oui, elles sont effectivement impossibles à « tracer » ou presque. Les cybercriminels ne s'y trompent pas, qui demandent aux victimes rançonnées de payer en bitcoins, ce qui les protège. Cela protège cependant aussi les victimes : un versement par carte bancaire à une mafia d'un pays de l'Est n'est pas une très bonne idée. Certains opérateurs sont sollicités par des clients qui leur demandent tout simplement comment ils peuvent payer une rançon en bitcoins. Je suis incapable de vous dire à quel point les crypto-monnaies peuvent déstabiliser l'économie – ce n'est pas mon métier, mais il est certain qu'elles entrent dans le paysage de la cybercriminalité, et il n'y a pas de raison que cela s'arrête.

Qu'en est-il de la vulnérabilité des opérateurs d'importance vitale ? La situation est très hétérogène. Certains sont très sérieux ; je pense à ceux qui s'occupent des centrales nucléaires, avec qui nous travaillons en lien étroit depuis des années – je ne suis pas inquiet. Il faut cependant considérer l'ensemble de la chaîne. À l'autre extrémité, il y a des compteurs intelligents qui sont autant de cibles potentielles. C'est l'ensemble de la chaîne qu'il faut protéger, pas uniquement les points les plus dangereux apparemment ni les plus symboliques.

Nous avons encore beaucoup de travail. Une approche réglementaire fait gagner beaucoup de temps et me paraît pertinente. L'extension de la démarche aux opérateurs de services essentiels, au-delà des 200 OIV, nous permettra également d'aller plus loin.

Avec la sonde souveraine de Thales – il en est d'autres –, nous revenons à la thématique de la détection. Nous imposons aux opérateurs d'importance vitale de faire de la détection, de recourir à des prestataires de détection. Évidemment, si c'est mal fait, ce sera une fragilité supplémentaire. Si certains grands acteurs et prestataires, que l'on qualifie au nom du Premier ministre, tels Thales, Airbus et Atos, se mettent à faire de la détection d'attaques pour de nombreux clients très sensibles, les attaquants s'en prendront demain non plus aux clients mais aux prestataires, car c'est là qu'ils pourront indirectement accéder aux

informations qui les intéressent. Il est donc très important que le niveau de sécurité de ces prestataires soit extrêmement élevé. C'est l'intérêt de la qualification, et de la vie dure que nous leur menons – nous avons une très bonne relation avec eux, mais je sens bien que nous les fatiguons un peu. Il faut que la sonde elle-même, qui détectera les menaces, soit de confiance, et qu'un attaquant ne puisse en modifier le fonctionnement. C'est la raison pour laquelle nous avons besoin dans les cas les plus sensibles de sondes dites « souveraines », car nous ne pouvons exclure la possibilité que des sondes étrangères soient aveugles à une partie des menaces. Dans des cas moins sensibles, nous pouvons faire des compromis et recourir à d'autres sondes.

La relation que l'ANSSI et l'ARCEP entretiendront sera différente, effectivement, mais parlons tout de suite de l'avis de l'ARCEP. Il porte sur une version très primitive du texte – dont témoigne la mention d'articles 19 *bis*, 19 *ter*, etc. Le problème est donc qu'il s'agit d'un avis sur un texte qui n'est pas connu. Le texte actuel tient compte de nombre des remarques de l'ARCEP.

Nous continuons évidemment à parler avec eux, en bonne intelligence. L'idée est d'établir un contrôle efficace mais également raisonnable. Par exemple, nous ne voulons pas d'un contrôle *a priori*. Il faut un contrôle efficace, global, qui permette d'éviter des dérives et de nous arrêter si nous allons trop loin – c'est normal. Aujourd'hui, par peur d'aller trop loin dans l'exercice de nos missions actuelles, nous nous autocensurons parfois. Il nous manque une capacité de contrôle. J'accueille donc avec plaisir le contrôle de l'ARCEP dont je pense qu'il nous fera gagner en efficacité. Ce n'était pas le cas lorsque nous nous construisions mais, maintenant que nous nous installons dans le paysage et que nous commençons à faire beaucoup de choses, l'absence de contrôle nous freine.

L'article 19 n'est probablement pas suffisant. Une thématique n'est pas abordée ici : la possibilité d'une démarche plus active. Il n'y a là nul motif de honte ; simplement, nous ne sommes pas prêts. Aussi ne faisons-nous aujourd'hui que de la détection, nous ne pouvons arrêter une menace. Demain, peut-être – je prends des précautions parce que c'est beaucoup moins anodin –, nous demanderons aux opérateurs de communications électroniques d'arrêter certaines attaques, de les bloquer. Cela rouvre cependant immédiatement le débat sur la neutralité du net, à laquelle nous ne portons présentement pas atteinte. Seuls les opérateurs seraient en effet en mesure d'arrêter certaines attaques, telles les attaques par déni de service (DDoS attack, *distributed denial of service attack*) : un attaquant prend le contrôle de très nombreuses victimes primaires, qui ne s'en rendent même pas compte, et, ensuite, toutes s'en prennent à une cible, ce qui la sature complètement et la bloque. Les machines contrôlées peuvent être des ordinateurs, des objets connectés ou même des caméras de surveillance. Je prends là l'exemple emblématique d'une attaque survenue il y a un an : l'attaquant, ayant pris le contrôle de ces caméras, a pu faire tomber un important opérateur américain, Dyn, et, pendant plusieurs heures, des services comme Netflix ont été totalement bloqués. Il est très dur d'agir à la source de l'attaque, par définition très « distribuée », et il est impossible de faire quoi que ce soit au niveau de la victime, submergée – OVH a également été attaqué de la sorte. Il n'y a que les opérateurs, entre la source et la cible, qui pourraient faire quelque chose, mais nous nous l'interdisons pour l'instant, car nous ne sommes pas prêts. Il faut pouvoir proposer un dispositif à la fois efficace et protecteur, qui ne puisse entraîner des dérives. Si l'avis de l'ARCEP évoque la neutralité du net, c'est parce que le texte initial prévoyait des éléments de ce type, actifs, mais ils en ont été retirés.

Mme Émilie Guerel. Au mois de juin 2017, vous aviez exprimé, dans une interview, une volonté de recourir à des prestataires privés, tant pour les audits et la détection que pour réparer les systèmes infectés. L'idée était que l'ANSSI puisse, à terme, se consacrer aux cas les plus graves et les plus atypiques, le traitement des cas les plus classiques étant dévolu aux prestataires. Ce souhait est-il toujours d'actualité ? Est-ce un objectif à atteindre au cours des prochaines années ?

M. Olivier Becht. Dans le cyberespace, le match en train de se jouer – vous l'avez bien montré – opposera une fois de plus le bouclier et l'épée. En l'occurrence, c'est la puissance de calcul qui fera le vainqueur. Comment évaluez-vous les efforts prévus par la LPM ? Je songe notamment au quantique. Le montant des études amont passe de 730 millions à un milliard mais une part déterminée doit-elle être consacrée à la puissance de calcul ?

M. Thomas Gassilloud. Que pensez-vous de l'utilisation par l'État de suites logicielles non souveraines ? Finalement, peu importe que le réseau soit sécurisé, si le logiciel utilisé ne l'est lui-même pas.

En matière de lutte antiterroriste, la Direction générale de la sécurité intérieure, par exemple, a signé en 2016 un contrat de 10 millions avec Palantir, startup financée par la CIA. À l'époque, il était indiqué qu'aucune entreprise française ne disposait d'une telle solution. La LPM insiste sur la nécessité de disposer d'un système de systèmes. La Direction générale de l'armement conduit le programme ARTEMIS - – architecture de traitement et d'exploitation massive de l'information multi-source – pour exploiter les bases de données de toute nature et un premier démonstrateur devrait être disponible en 2019 ou 2020.

Que pensez-vous donc de l'utilisation par l'État de suites logicielles non souveraines ? Êtes-vous impliqué dans le programme ARTÉMIS ? Plus globalement, comment faire pour que les investissements de défense en matière logicielle contribuent au renforcement de notre souveraineté numérique ?

M. Loïc Kervran. Tout d'abord, je me réjouis de ce que vous avez annoncé à propos de l'article 20, car la situation n'était pas satisfaisante.

Selon mes informations, il y a déjà des sondes et des marqueurs techniques chez un certain nombre d'opérateurs. L'ARCEP estime d'ailleurs que le cadre légal en vigueur le permet déjà et que la LPM n'apporte pas grand-chose – je précise d'ailleurs que l'ARCEP n'a pas fondamentalement changé d'opinion depuis la publication de l'avis.

Vous avez évoqué les différences entre métadonnées et contenu, mais des personnes relativement qualifiées, à la direction technique de la DGSE, par exemple, considèrent aujourd'hui qu'il est très difficile de faire la distinction sur le net. Prenez une URL : au début, ce sont surtout des données techniques ; à la fin, le mot-clé relève plutôt du contenu. C'est donc beaucoup plus compliqué qu'en matière de communications téléphoniques.

Par ailleurs, je ne vois pas du tout, dans ce texte, le lien entre le défensif et l'offensif – même quand l'action offensive ne vise finalement qu'à protéger. Il n'est pas non plus question de l'attribution des attaques. J'ai quand même du mal à imaginer que l'on ne va pas réagir et qu'on ne cherchera ni à l'attribuer à un auteur ni à la stopper.

Quant aux sondes vues comme sources de fragilité, les opérateurs peuvent placer les sondes qu'ils souhaitent sans même en informer l'ANSSI. Ne faudrait-il pas modifier le texte sur ce point ? Ou alors s'agit-il de sondes qui ne présentent pas de risque particulier ?

M. Guillaume Poupard. Je commencerai par répondre à la question relative aux prestataires qualifiés. Aujourd'hui, l'ANSSI invente – c'est son rôle – certains métiers autour de l'audit, de la réaction aux incidents informatiques et de leur détection. Nous inventons des processus, parce qu'il n'existe aucun manuel ancien expliquant comment faire ces métiers. En revanche, nous sommes incapables d'exercer ces métiers auprès de l'ensemble des victimes à protéger. Même en se cantonnant aux victimes les plus sensibles, en commençant par les opérateurs d'importance vitale, l'ANSSI n'a pas les moyens de protéger tout le monde – et ne les aura pas, car ce ne serait pas une bonne chose. Nous avons choisi un modèle consistant à développer des compétences, à assurer leur maîtrise en interne, et à encourager des prestataires privés de confiance à développer les mêmes métiers.

C'est là qu'intervient la question de la qualification, qui est un acte d'évaluation fondé sur un référentiel public auquel des entreprises se soumettent volontairement pour, le cas échéant, obtenir *in fine* une qualification que je délivre au nom du Premier ministre dans les métiers d'audit, de détection et de réaction aux incidents – étant entendu que nous allons continuer d'enrichir la palette des métiers. Il en résulte à l'évidence un effet de levier. Incidemment, le problème du financement est en partie résolu, ces métiers de l'audit et de la détection de haut niveau ayant un coût ; ils relèvent en l'occurrence du domaine des contrats privés. Je n'impose jamais à un quelconque opérateur d'importance vitale ou autre de travailler avec tel ou tel partenaire ; il appartient à chacun d'entre eux de choisir le prestataire qualifié – c'est-à-dire fiable et compétent – qui convient à la mission recherchée.

L'ANSSI peut ainsi, avec ses moyens propres qui, quoique non négligeables, sont clairement bornés, se concentrer sur les cas les plus sensibles dans lesquels il n'est pas souhaitable de recourir à un prestataire privé – je pense à certains cas étatiques – et sur des cas nouveaux qu'il faut défricher pour inventer de nouveaux métiers. Les auditeurs de l'ANSSI, par exemple, qui savent faire le travail des attaquants et sont donc capables de tester la vulnérabilité des systèmes, effectuent des inspections ministérielles – un champ que nous préférons maintenir au niveau étatique – ou examinent des systèmes atypiques dont nul ne sait encore vraiment comment vérifier le niveau de sécurité. Une fois la connaissance acquise, ils la transfèrent aux prestataires privés qualifiés.

En matière de puissance de calcul, il existe une asymétrie totale entre les attaquants et les défenseurs. Les attaquants n'ont pas besoin – du moins pas encore – de puissance de calcul : une attaque ne nécessite que des moyens très simples et ne coûte presque rien. Pour se défendre, en revanche, nous avons un besoin croissant de puissance de calcul – ainsi que pour les actions de cryptanalyse, qui relèvent pour l'essentiel de la DGSE. De même, l'ordinateur quantique servira principalement à déchiffrer des communications.

L'ANSSI qui, étant un service du Premier ministre, n'est pas directement concernée par le volet programmatique de la LPM, achève actuellement la construction d'un centre de données de très grande taille pour anticiper la transformation de notre métier. Nous allons en effet devoir traiter et conserver un volume croissant de données techniques, ou métadonnées, en provenance notamment des sondes placées dans les ministères. La conservation des données n'est pas un but en soi et ne répond pas un objectif de renseignement ; elle sert

simplement à pouvoir remonter dans le temps. Or, la conservation de téraoctets de données et la capacité à les fouiller pour vérifier si une menace nouvelle est déjà apparue dans le passé ont un coût et nécessitent de véritables capacités de calcul. Cela étant, je ne peux pas vous dire si la LPM est adaptée de ce point de vue.

Le débat sur la souveraineté des logiciels est récurrent. Soyons clairs : il n'est heureusement pas nécessaire, pour bâtir un système souverain, que tous ses composants soient souverains eux aussi – chose que nous n'avons jamais su et ne saurons jamais faire. Il faut donc accepter que des microprocesseurs, des ordinateurs ou des logiciels ne soient pas totalement maîtrisés – dans le cas contraire, le coût serait délirant. Dans certains cas – je me fonde en l'occurrence sur mon expérience à la direction générale de l'armement – nous identifions des briques, qu'il s'agisse de logiciels ou de matériels, qui doivent impérativement être maîtrisés : mieux vaut par exemple ne pas acheter un composant de chiffrement dans un chiffreur gouvernemental ailleurs que chez un industriel en qui nous avons une totale confiance, voire, en pratique, le fabriquer en étroite coopération avec l'industriel en question.

Puis se pose la question de l'assemblage et de l'intégration des briques maîtrisées avec d'autres briques qui ne le sont pas ou peu afin de bâtir un système globalement sûr. Contrairement à une idée simple mais courante, la sécurité d'un système ne se réduit pas à la sécurité de son maillon le plus faible, car un système complexe ne se réduit pas à une simple chaîne. En jouant sur l'architecture et la conception même des systèmes, il est possible d'intégrer des composants qui ne sont pas maîtrisés en toute confiance – encore faut-il être capable d'effectuer ce travail architectural. De ce point de vue, de nombreux industriels de l'armement vivent une révolution depuis quelques années : ils étaient jusqu'à récemment d'avis que la partie logicielle ne les concernait pas, et voilà qu'ils se transforment de plus en plus souvent en éditeurs logiciels. Hervé Guillou aime à dire qu'un bateau est désormais constitué de 50 % de logiciels et de 50 % de chaudronnerie, la seconde part étant destinée à poursuivre sa diminution au profit de la première. Or, tous les logiciels d'un bateau ne peuvent pas être maîtrisés.

On peut certes s'interroger sur certains logiciels comme ceux de Palantir ; de même, l'ombre de la suite Microsoft plane à chaque fois que l'on parle de logiciels souverains. L'essentiel est de disposer d'une architecture globale qui permette d'utiliser ces logiciels de manière précautionneuse. Il va de soi qu'il faut par exemple déconnecter les logiciels Palantir, qui permettent d'effectuer des recherches dans les données, car il est hors de question que l'éditeur de Palantir ait accès aux données opérationnelles traitées par le logiciel. Or, c'est de plus en plus compliqué : de nombreux éditeurs logiciels, en effet, dégagent leur plus-value en fournissant non plus un simple CD-ROM comme autrefois mais un système à distance, en *cloud*, qui, pour fonctionner, ne doit plus se trouver chez le client mais chez l'éditeur, ce qui soulève de nombreuses questions. S'agissant de Palantir, il existe une volonté globale de créer une alternative française de confiance, et la DGA y travaille. Quant au programme d'études amont (PEA) ARTEMIS, l'ANSSI y consacre une part substantielle de ses moyens et entretient à cet égard des liens de confiance étroits avec la DGA.

Je conclurai néanmoins par une note quelque peu pessimiste : en toute objectivité, le développement logiciel n'est pas le point fort de la France et ne l'a jamais été. C'est ce qui justifie l'idée que nous avons eue, en commun avec la DGA et la direction générale des entreprises de Bercy, de nous concentrer sur les sujets critiques plutôt que de chercher à redévelopper en France tous les types de logiciels, ce que nous ne parviendrions pas à faire.

J'en viens à la sécurité des sondes des opérateurs. Avant même de songer à installer de nouvelles sondes, il faut exploiter celles dont ils disposent. En réalité, les opérateurs sont déjà très actifs pour détecter les menaces qui les visent, car ils sont obsédés par la protection de leur système central, leur *backbone*. Les opérateurs d'importance vitale ont non seulement le droit mais l'obligation de se doter de systèmes de détection qualifiés et de haut niveau pour se protéger eux-mêmes. Disons, en guise d'analogie, qu'il s'agit de rendre les tuyaux complètement étanches afin qu'ils ne polluent surtout pas l'opérateur lui-même bien qu'ils transportent n'importe quoi, la qualité de l'eau ainsi transportée n'étant pas contrôlée. C'est précisément la qualité de l'eau que nous voulons désormais examiner. Encore une fois, les réseaux propres des opérateurs, eux, sont normalement déjà couverts ; nous travaillons avec eux depuis longtemps et procédons à des inspections pour vérifier la sécurisation de leurs *backbones*, par crainte d'une attaque qui provoquerait l'effondrement de leurs systèmes, ce qui produirait des effets en cascade dramatiques – raison pour laquelle je place les opérateurs de communications électroniques sur le même plan que l'énergie et les transports en ce qui concerne le caractère prioritaire de la prise en compte de la menace car, quoique moins spectaculaire, la perte des télécoms et d'internet aurait des effets terribles.

Je ne suis pas entré dans le débat relatif aux métadonnées.

M. Loïc Kervran. Un peu tout de même, en employant l'image du livre scanné dans un aéroport !

M. Guillaume Poupard. En l'occurrence, cette image a trouvé ses limites… Les adresses IP sont des données personnelles, mais l'ANSSI perdrait sa raison d'être si elle s'interdisait de les traiter. Elles constituent en effet le fonds de commerce du centre opérationnel. Selon la jurisprudence de la DGSE et, surtout, de la Commission nationale de contrôle des techniques de renseignement (CNCTR), une URL – une adresse de site internet – est une donnée signifiante, et non une métadonnée. Parmi les marqueurs techniques que nous utilisons se trouvent donc des URL : lorsque nous identifions un site Internet clairement malveillant, son adresse internet est l'un de ses marqueurs les plus triviaux, que nous souhaitons pouvoir partager avec les opérateurs de communications électroniques.

Il va donc de soi que nous traitons des données, y compris des données personnelles. C'est pourquoi le texte ne loi ne saurait comprendre une disposition visant à rassurer qui interdirait de toucher aux données personnelles : nous y touchons de fait. L'essentiel est que la finalité reste la détection et que l'on s'en tienne aux données strictement nécessaires et signifiantes. Prenons un exemple : le travail de détection consiste parfois à chercher au fin fond de pièces jointes, dans des courriers électroniques, pour y détecter un éventuel virus caché. Le virus en question n'est pas une donnée signifiante pour l'utilisateur, qui ne le voit pas ; l'ANSSI, quant à elle, entre dans la pièce jointe pour trouver le virus mais n'affiche à aucun moment le contenu de la pièce qui, pour elle, n'a aucun sens.

Ce débat peut être complexe. Disons qu'il est hors de question de cibler la donnée signifiante pour la victime, mais plutôt la donnée signifiante pour l'attaquant, c'est-à-dire les pièges et virus parfois dissimulés dans les plus lointains recoins d'une pièce jointe. Or, pour être efficace, il faut souvent se rendre jusque dans ces recoins et, pour ce faire, être capable de reconstituer les pièces jointes concernées – d'où les discussions sur l'inspection des paquets en profondeur, *deep packet inspection* (DPI), qui inquiète légitimement. Sur le plan technique, comme je l'ai indiqué peut-être trop franchement aux journalistes qui maîtrisent ces questions,

cette méthode ressemble à la DPI même si sa finalité diffère et que les produits de DPI à des fins de renseignement ne fonctionnent pas de la même manière. En tout état de cause, il faut bien, à un moment ou à un autre, aller voir de quoi il s'agit car les attaquants, eux, iront là où ils se savent indétectables, de même qu'ils utilisent aujourd'hui des hébergeurs français, conscients que la France ne sait pas vérifier si un serveur a été infecté ou non. Nos partenaires étrangers nous alertent d'ailleurs sur la recrudescence incroyable d'infections de serveurs en France, qui est liée au fait que les attaquants suivent de près l'évolution de la réglementation des différents pays – ce qui n'est guère difficile.

L'article 19 n'aborde pas la question du lien offensif-défensif et de l'attribution car ce n'est pas son objet. Cela ne veut pas dire que nous ne faisons rien, loin s'en faut. La question de l'attribution – identifier qui attaque – relève clairement des services de renseignement, même si le pouvoir judiciaire peut jouer un rôle. En pratique, il est extrêmement difficile d'établir avec certitude l'identité de l'attaquant. L'ANSSI, en revanche, peut déterminer techniquement si deux attaques sont conduites par la même personne ou par le même groupe, car les mêmes méthodes et outils seraient utilisés. En revanche, elle ne peut pas établir si le groupe en question est russe, chinois, américain ou autre. Des indices peuvent exister – un code d'attaque comportant des caractères cyrilliques utilisé par un attaquant travaillant aux heures de Moscou, par exemple. Ce ne sont pourtant que des indices, et non des preuves : il est très simple pour un attaquant non russe d'insérer du cyrillique – certains le font très bien – dans ses codes d'attaque et de se lever en pleine nuit pour travailler aux heures de Moscou. Seuls les services de renseignement peuvent apporter à un tel faisceau d'indices des éléments vraiment crédible – ce qu'ils commencent à faire plutôt bien, même s'il s'agit d'un axe de progrès majeur. Les moyens consacrés à la cyberdéfense dans la LPM vont précisément dans cette direction.

La France a fait le choix de dissocier les missions offensives et les missions défensives. Il est clair pour tous – les agents, Patrick Pailloux, moi-même – que chacun a sa mission à l'abri de tout conflit. Que les missions soient dissociées, cependant, ne signifie pas que nous n'avons pas le droit de nous parler, notamment de l'articulation qui existe entre la détection, l'aide aux victimes, l'attribution voire, à l'avenir, la contre-offensive – par laquelle on ne saurait pas commencer car, avant de contre-attaquer, il faut connaître l'attaquant. Il va de soi qu'il faut trouver cette articulation et, de ce point de vue, le système français me semble bien conçu : les missions sont séparées mais la proximité entre les services est assez grande, ne serait-ce qu'en raison du chapeau du Premier ministre, pour que nous travaillions tous ensemble, chacun dans son domaine de compétence.

Il me reste à répondre au sujet des sondes...

M. Loïc Kervran. En effet, les opérateurs peuvent désormais placer leurs propres marqueurs. Or, vous avez dit que les sondes elles-mêmes peuvent constituer une source de vulnérabilité des réseaux. Faut-il donc que les marqueurs des opérateurs soient contrôlés ?

M. Guillaume Poupard. L'ARCEP s'en chargera, ne serait-ce que parce qu'elle est la seule à comprendre quoi que ce soit à ce que font les opérateurs.

M. le président. Nous veillerons à l'inscrire au compte rendu…

M. Guillaume Poupard. C'est tout à l'honneur de l'ARCEP ! Disons qu'un cœur de réseau moderne est une usine d'une complexité incroyable.

La détection par un SOC – *Security Operations Center* –, c'est-à-dire un système de supervision, devient un centre névralgique qu'il faut protéger, comme il faut protéger le centre de planification et de conduite des opérations (CPCO) dans le domaine militaire. En effet, si un attaquant lit à livre ouvert dans les intentions du CPCO, il sera très difficile de conduire des opérations efficaces.

Encore une fois, la priorité pour les opérateurs n'est pas de déployer des sondes partout mais d'exploiter les données dont ils disposent déjà, c'est-à-dire d'y rechercher des marqueurs connus – ce qui n'est pas encore fait systématiquement – mais aussi des marqueurs qui ne sont pas connus et que nous ne voulons pas rendre publics. On me fait parfois le reproche de ne pas rendre publiques toutes les connaissances que nous avons des attaques mais si l'on annonce publiquement, y compris aux attaquants, qu'ils sont repérés, alors ils changeront immédiatement de méthode – et ils font preuve à cet égard d'une agilité incroyable. Il est donc normal, hélas, qu'une partie des marqueurs dits indicateurs de compromission (IOC) soient publics et exploités, mais que le secret entoure encore, à des degrés parfois très élevés, certains marqueurs si précieux et sensibles que nous ne voulons pas les donner – le problème étant qu'ils se trouvent dans nos coffres et qu'ils ne détectent rien. Il nous faut donc trouver un équilibre entre les marqueurs que nous pouvons donner à certains opérateurs de confiance et les sondes souveraines, qui ont tout leur rôle à jouer parce qu'elles sont capables de garder le secret concernant les marqueurs techniques qu'il ne faut pas révéler aux attaquants.

M. Bastien Lachaud. Ma première question a trait aux données personnelles de nos concitoyens et aux GAFA – pour Google, Apple, Facebook, Amazon. Dans la revue stratégie de défense et de sécurité nationale, ce point est considéré comme une vulnérabilité. D'ailleurs, pour s'en prémunir, la Russie stocke la totalité des données personnelles de ses citoyens sur son territoire. Or, la LPM ne comprend aucune disposition à cet égard. Quelle serait selon vous la réponse française adaptée face à cette vulnérabilité ?

D'autre part, nombreux sont les habitants de ma circonscription qui s'interrogent sur Enedis, que vous assistez pour l'installation des compteurs Linky qui suscitent un véritable débat démocratique. À quel niveau aidez-vous Enedis ? Quels éléments d'information pouvez-vous nous donner à ce sujet ?

Mme Nicole Trisse. N'y a-t-il pas besoin de développer des systèmes informatiques d'État afin de préserver l'ensemble de nos données et d'assurer la sécurité du pays ? En clair, que penseriez-vous d'un *Patriot Act* à la française ?

M. Jean-François Eliaou. Nous n'avons pas abordé la relation qui existe entre l'ANSSI et le COMCYBER, sur laquelle le général Bonnet de Paillerets nous a récemment donné quelques éléments de son point de vue. Qu'en est-il du vôtre ?

M. Philippe Michel-Kleisbauer. Je vous poserai ma question favorite, Monsieur le directeur général : devons-nous dénier à d'autres États la capacité de se doter d'une cyberdéfense pour se protéger, comme nous l'avons fait en matière nucléaire, en réservant l'accès à certaines technologies à un groupe fermé de puissances ?

M. Guillaume Poupard. Je pourrais esquiver la question sur les données personnelles en vous renvoyant vers la CNIL, mais ce serait trop facile. De fait, le règlement général sur les données personnelles en cours de déploiement constitue une avancée majeure.

Est-elle suffisante ? Je l'ignore. A-t-elle un impact ? Est-elle lourde ? Oui, à l'évidence. Toutes les sociétés que je rencontre paniquent à l'idée de sa mise en œuvre. Nous allons donc dans le bon sens en Europe et même au-delà.

À titre personnel, je dirais que les GAFA et autres sont dans le paysage, et toute solution simple qui consisterait à les interdire n'aurait pas de sens. La solution, forcément complexe, passe par la sensibilisation et l'explication. Il arrive d'ailleurs que j'explique les choses de manière assez brutale à certains acteurs économiques, pour leur faire comprendre leur irresponsabilité de confier tous leurs systèmes à Google – ce que certains font – mais ils ont beau jeu de me répondre que ces systèmes fonctionnent bien et ne coûtent pas cher. En clair, nous devons mener un dialogue et ce dialogue, parfois, se tend jusqu'à remonter aux plus hautes autorités de l'État de sorte qu'elles montrent les gros yeux pour faire plier tel ou tel acteur, étant entendu que cette méthode ne peut être réservée qu'à quelques cas et ne saurait être généralisée. Objectivement, la situation est compliquée, notamment par manque de prise de conscience. Au-delà des attaquants bien identifiés qui représentent une menace évidente, je constate encore un manque de lucidité concernant le risque que présentent les grandes sociétés numériques, en particulier américaines, à qui l'on prête parfois une image trop bonne. Quoi qu'il en soit, c'est par la discussion qu'il faut procéder et l'ANSSI n'est qu'un petit maillon dans cette chaîne – raison pour laquelle je suis un peu gêné de vous répondre.

Sur Linky, en revanche, je serai beaucoup plus à l'aise. Tout d'abord, la CNIL a largement réglé la question de savoir si cet outil permettait ou non d'espionner la vie des gens. Ensuite, je laisse aux spécialistes médicaux le soin d'apprécier si les ondes émises par les compteurs sont cancérigènes, mais j'en doute.

Nous avons dialogué avec les promoteurs de Linky dès l'origine du projet de compteur intelligent. Dans la chaîne des acteurs de l'énergie – les centrales nucléaires venant spontanément à l'esprit en premier –, il faut sécuriser tous les maillons, et les compteurs, quoiqu'en bout de chaîne, en font partie. Les compteurs d'hier étaient vulnérables : le plus souvent, ils se trouvaient dans la rue et il était facile de les détruire. La nouveauté symptomatique de l'informatique tient au fait qu'un individu pourrait non pas même espionner mais surtout éteindre tous les compteurs Linky d'une ville ; c'est le risque à redouter. Même en faisant toute confiance à nos énergéticiens, l'arrêt simultané de tous les compteurs risque de créer un excédent d'énergie et, sans doute, une rupture du réseau quelque part. Quoi qu'il en soit, il faut protéger ces compteurs.

À l'époque, il existait donc deux possibilités : signaler les risques et laisser l'opérateur s'en débrouiller ou l'aider. L'ANSSI a choisi à juste titre d'aider Enedis, ce que nous continuons de faire en apportant des conseils et en mettant à disposition notre mécanisme de certification de produits. C'est ainsi que tous les compteurs intelligents qui ont été déployés ont été évalués par des centres d'évaluation de la sécurité des technologies de l'information (CESTI) agréés par l'ANSSI. Chaque compteur est donc assorti d'un certificat que j'ai signé au nom du Premier ministre et qui atteste que son niveau de sécurité est satisfaisant en fonction de la cible de sécurité envisagée. C'est un travail colossal qui ne plaît pas à tout le monde, parce que certains produits ont été certifiés mais beaucoup ne l'ont pas été – avec des conséquences parfois dramatiques pour certains fabricants qui n'ont pas réussi à sécuriser leurs compteurs. Au vu des résultats, cependant, je ne prends pas la responsabilité, au nom du Premier ministre, de garantir la sécurité de tels produits ; ce ne serait pas

raisonnable. En revanche, les produits certifiés nous semblent atteindre un niveau satisfaisant – même si rien n'est jamais sûr à 100 % – compte tenu des risques identifiés. Tout cela constitue un équilibre subtil. Sachez toutefois que nous avons analysé et pris en compte la menace lors du développement technique des compteurs et de l'ensemble du système sur lequel ils sont assis. Je tiens plutôt à saluer l'intelligence et la qualité du travail considérable qu'ont accompli les équipes chargées de déployer les compteurs Linky – malgré d'inévitables frottements occasionnels.

M. Bastien Lachaud. La mise à jour des compteurs est-elle assurée ?

M. Guillaume Poupard. L'examen de la sécurité d'un produit porte non seulement sur la sécurité du produit initial, mais aussi sur celle de son environnement de développement avant même sa fabrication, et sur celle de tout son cycle de vie. Il est évidemment hors de question de certifier un produit qui serait initialement bon et qui serait ensuite mis à jour de manière aberrante pour devenir un mauvais produit. Le risque est limité s'agissant d'un compteur mais le système d'un gros opérateur de télécommunications, par exemple, est mis à jour quotidiennement. C'est ce qui explique pourquoi il est si difficile d'en préserver la sécurité dans le temps.

S'agissant du développement de systèmes d'État, Madame Trisse, des projets intéressants sont déjà en cours. Nous travaillons notamment avec la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), une sorte de direction des systèmes d'information de l'État qui dépend elle aussi du Premier ministre. Nous basculons par exemple vers un réseau interministériel de l'État destiné à innerver tous les ministères. Nous sommes de fervents partisans de ce genre d'actions, qui renforcent considérablement l'efficacité de la détection.

Plus généralement, vous soulevez la question des centres de stockage des données. Pendant assez longtemps, certains industriels étrangers non européens nous ont expliqué que la construction de nos propres centres de données n'avait aucun sens – et d'aucuns les ont crus. Ce n'est pas acceptable. Selon moi, il faut à l'évidence faire revenir les données personnelles en Europe, car on sait bien que les lois étrangères, américaines notamment, n'assurent pas la sécurité de données européennes stockées aux États-Unis ou ailleurs. Se pose ensuite la question de l'application extraterritoriale du droit américain : des données stockées en Irlande sur des serveurs appartenant à des industriels américains, par exemple, ne sont pas non plus totalement en sécurité. Il peut donc être envisagé de développer des espaces de stockage à distance – en *cloud* – et des centres de stockage pour des applications spécifiques. Une fois encore, je pense que pour de nombreuses applications, le périmètre adapté est européen ; dans certains cas, ayons même le courage de dire que les données doivent rester en France.

C'est le cas des informations classifiées de défense. Cela peut paraître une évidence, mais il faut s'assurer que les différents textes que l'on négocie le prévoient bien. Il peut s'agir d'une exception au principe de la libre circulation des données, *free flow of data*. Nous sommes très favorables à la libre circulation au niveau européen, mais il faut prendre garde aux risques qu'elle fait peser sur la sécurité au-delà de l'Union.

Je ne suis pas certain qu'il faille promouvoir l'idée d'un *Patriot Act* à la française. Il s'agit plutôt de constituer une plaque européenne, cohérente en termes de valeurs et de droits,

et suffisamment grande pour que l'on ne soit pas tenté de laisser les centres de données de l'autre côté de l'Atlantique, ce qui serait un non-sens technologique.

Nous entretenons des liens très étroits avec le COMCYBER. Les structures, et les hommes, s'entendent très bien depuis fort longtemps, ce qui est plutôt rassurant !

Le schéma est simple : il y a une seule autorité nationale, l'ANSSI. Mais, ainsi que je l'ai dit à plusieurs reprises, les moyens de cette autorité nationale unique sont limités. Par conséquent, je ne veux surtout pas les gaspiller là où existent déjà des compétences et des moyens. C'est bien le cas du ministère des Armées qui dispose de moyens et de compétences réelles, et a développé notamment des chaînes internes pour la sécurité informatique. Je préfère que les moyens de l'ANSSI soient concentrés vers d'autres ministères, moins armés – voire pas du tout – ou d'autres acteurs, notamment les OIV.

En pratique, l'ANSSI délègue certaines de ses activités, notamment d'audit et de détection, au COMCYBER – pour commandement de cyberdéfense. Le centre névralgique de la lutte informatique défensive, le CALID (Centre d'analyse de lutte informatique), tête de pont du COMCYBER, est logé dans la tour Mercure, au même étage que le centre opérationnel de l'ANSSI. Ces personnels ne peuvent être plus proches, à l'image d'un centre de contrôle aérien, où les contrôleurs civils contrôlent l'espace civil et les contrôleurs militaires, l'espace militaire, mais tournent leur siège et se parlent lorsqu'un avion passe d'un espace à l'autre. C'est, depuis le départ, le modèle un peu naïf que je promeus, avec le ministère des armées. Chacun a son domaine. Le COMCYBER traite de la question des réseaux nationaux, des réseaux en opérations extérieures (OPEX), des systèmes d'armes, ce qui exige beaucoup de ressources et de compétences, mais le jour où il y a un problème, nous sommes capables de reporter notre expertise et notre énergie. L'ANSSI vient en support si des réseaux dépendant du ministère des Armées sont attaqués. Les sondes utilisées par le COMCYBER, opérées par le CALID, ont été développées par l'ANSSI. Ce n'est pas à proprement parler de l'intégration, mais un niveau de coopération très élevé. Nous comptons, avec Olivier Bonnet de Paillerets, développer encore cette coopération pour éviter des redondances inefficaces et surtout des trous dans la raquette.

Au niveau européen, la directive NIS, prévoit que les États s'efforcent d'assurer un niveau de sécurité élevé, en fonction de leurs compétences et de leurs moyens, et que ces capacités fonctionnent en réseau. Nous ne croyons pas à un modèle européen, ou otanien, où des grandes puissances apporteraient une protection cyber aux autres États, d'abord parce qu'il existe des questions de souveraineté nationale, ensuite parce que certains domaines ne relèvent pas du militaire. Ainsi, nous nous sommes toujours opposés à ce que l'OTAN puisse s'occuper de la sécurité bancaire. La tentation existe, mais ce n'est pas le métier de l'OTAN Et il y a une ligne rouge à ne pas franchir. En revanche, chaque pays doit développer sa sécurité bancaire, les opérateurs bancaires assurer leur propre sécurité et ainsi de suite.

Tout cela doit fonctionner en réseau, et c'est un domaine où nous devons encore faire des progrès. Trop souvent, l'information est connue, mais elle n'est pas partagée, parce que c'est compliqué. Nous y mettons beaucoup d'énergie : les centres opérationnels qui gèrent ces questions de cybersécurité, les CERT – *Computer Emergency Response Team* – ou CSIRT – *Computer Security Incident Response Team* – ont vocation à travailler en réseau. En France, il s'agit du Centre opérationnel de la sécurité des systèmes d'information, le COSSI, et du CALID en matière militaire. Il faut y ajouter le centre technique de la capacité OTAN de

réaction aux incidents informatiques – NCIRC – et le CERT-EU, au niveau des institutions européennes.

Monsieur Michel-Kleisbauer, il serait totalement contre-productif de chercher à bloquer l'exportation de solutions défensives. Mais nous savons aussi, et les industriels nous le disent, que ces pays cherchent, certes à se protéger, mais surtout à attaquer. C'est là où le contrôle-export intervient : il s'agit de faire en sorte que les industriels vendent des systèmes défensifs, mais n'aident pas à développer les capacités offensives. Pour ma part, je suis très opposé à toute forme d'export qui pourrait faciliter la prolifération de technologies offensives.

Objectivement, la tâche est très difficile, dans un domaine qui relève de l'intangible, du savoir-faire. Certaines technologies défensives peuvent facilement être transformées. Je l'ai dit tout à l'heure, les auditeurs ont des compétences d'attaquant. Comment s'assurer que les auditeurs que l'on forme à la protection des systèmes d'information, dans un pays un peu louche, ne sont pas les embryons d'une capacité offensive ? C'est une question que nous discutons constamment et qui suppose une relation de confiance avec les industriels. Il est nécessaire aussi de faire évoluer le dispositif de contrôle à l'exportation, porté par le service des biens à double usage et par la commission interministérielle pour l'étude des exportations de matériel de guerre – CIEEMG. Ce qui fonctionne pour des biens matériels ne se transpose pas aisément dans un domaine aussi intangible.

M. le président. Merci, Monsieur le directeur général.

La séance est levée à douze heures cinquante.

*

* *

Membres présents ou excusés

Présents. - M. François André, M. Jean-Philippe Ardouin, M. Florian Bachelier, M. Thibault Bazin, M. Olivier Becht, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. Philippe Chalumeau, M. Jean-Pierre Cubertafon, Mme Marianne Dubois, Mme Françoise Dumas, M. M'jid El Guerrab, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Claude de Ganay, M. Thomas Gassilloud, M. Fabien Gouttefarde, Mme Émilie Guerel, M. Jean-Michel Jacques, M. Loïc Kervran, M. Bastien Lachaud, M. Fabien Lainé, M. Christophe Lejeune, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, M. Gwendal Rouillard, Mme Laurence Trastour-Isnart, Mme Nicole Trisse, M. Stéphane Trompille

Excusés. - M. Bruno Nestor Azerot, M. Luc Carvounas, M. André Chassaigne, M. Stéphane Demilly, M. Olivier Faure, M. Richard Ferrand, M. Marc Fesneau, M. Laurent Furst, Mme Séverine Gipson, M. Christian Jacob, M. Jean-Christophe Lagarde, M. Jacques Marilossian, Mme Natalia Pouzyreff, M. François de Rugy, Mme Sabine Thillaye, Mme Alexandra Valetta Ardisson

Assistaient également à la réunion. - M. Jean-François Eliaou, M. Olivier Gaillard