ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Mardi
16 juillet 2013
Séance de 17 heures 30

Compte rendu n° 86

SESSION EXTRAORDINAIRE DE **2012-2013**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de M. Philippe Nauche, *vice-président*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures trente.

M. Philippe Nauche, président. Je suis heureux d'accueillir au nom de la présidente de notre commission, qui s'excuse de ne pouvoir être parmi nous cet après-midi, M. Patrick Pailloux, directeur général de l'Agence de sécurité des systèmes d'information (ANSSI). Après avoir entendu le 12 juin dernier le contre-amiral Arnaud Coustillière, officier général chargé de la cyberdéfense à l'état-major des armées puis la semaine dernière, l'ingénieur en chef de l'armement Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la direction générale de l'armement, nous terminons ainsi notre cycle d'auditions consacrées à la cyberdéfense. Ces deux auditions nous ont permis de mesurer le chemin parcouru mais aussi ce qui reste à faire dans la prochaine loi de programmation militaire. Votre point de vue, monsieur Pailloux, sera nécessairement plus large que celui des deux acteurs du ministère de la Défense que nous avons reçus avant vous, car l'ANSSI s'intéresse à la cybersécurité dans son ensemble.

M. Patrick Pailloux, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI). Mesdames et messieurs les députés, je suis flatté d'avoir l'occasion de m'exprimer devant votre commission. Travaillant depuis longtemps dans les domaines de la cybersécurité et de la cyberdéfense, je suis malheureusement bien placé pour connaître la menace. Le contexte est si inquiétant que je suis heureux de toute occasion qui m'est donnée de sensibiliser la représentation nationale à ces problèmes.

La première des menaces informatiques est l'espionnage. Bien qu'il soit difficile de le mesurer, on peut affirmer que le cyber-espionnage n'a jamais été aussi important qu'aujourd'hui et dépasse, de loin, tout ce que l'on a pu connaître précédemment. En permanence, c'est vrai au moment même où je vous parle, de très grandes entreprises sont pillées par des pirates informatiques qui se sont introduits au sein de leurs réseaux depuis des semaines, des mois, voire des années – la durée moyenne d'observation dépasse un an – et, en toute impunité, leur volent leur patrimoine. Cela est arrivé aussi à des administrations, dont Bercy durant la présidence française du G 20. Cet espionnage n'est pas l'apanage de grands services de renseignement. Il est, hélas, à la portée d'un très grand nombre d'acteurs. De toutes petites officines peuvent se livrer à de l'espionnage simple, pour un coût ne dépassant pas quelques centaines d'euros.

La deuxième menace est la déstabilisation. Tout conflit, quel qu'en soit le lieu, la nature – sociale, politique, religieuse… –, la portée – locale, nationale ou internationale – et la forme, s'accompagne désormais d'attaques informatiques. Lors de l'opération Serval au Mali, des activistes opposés à l'intervention française ont lancé des cyberattaques pour manifester leur désapprobation. De même, le blog du Premier ministre a été piraté pour dénoncer le projet d'aéroport de Notre-Dame des Landes. Au même titre que les manifestations de rue, les attaques informatiques sont devenues un moyen d'exprimer une protestation. Ces attaques prennent trois formes essentielles. La première consiste à défigurer les sites Internet à des fins revendicatives : les attaquants affichent un message, souvent des plus vulgaires, sur la page d'accueil. La deuxième consiste à bloquer les sites en les saturant de trafic : c'est ce qui est arrivé en décembre 2011 au site du Sénat, bloqué par des pirates turcs en représailles du vote de la loi réprimant la négation du génocide arménien. C'est une forme de « cyber-sit-in ». Le troisième mode d'action consiste à pénétrer les systèmes d'information puis de rendre publiques les informations volées. Des opposants aux travaux du GIEC, le groupe

international d'experts sur le climat, ont ainsi révélé le contenu de sa messagerie, portant sur la place publique les débats internes au groupe de chercheurs pour tenter de les déconsidérer.

La troisième menace est le cyber-sabotage. Nos sociétés sont devenues dépendantes de l'informatique et des télécommunications. Ce sont des systèmes informatiques qui contrôlent la production et la distribution d'électricité, les réseaux de transports en commun, la climatisation des bâtiments, les systèmes de télécommunications… Toute attaque est susceptible de faire dysfonctionner ces systèmes et d'occasionner de sérieux dommages. Chacun imagine aisément les conséquences potentielles d'une attaque sur les commandes de contrôle d'un barrage par exemple. De tels sabotages ne sont, hélas, plus de la science-fiction. Les centrifugeuses iraniennes d'enrichissement de l'uranium ont été endommagées par le virus Stuxnet. La compagnie pétrolière saoudienne Aramco a elle aussi été victime d'une attaque. Et tout récemment, dans un contexte de tension entre la Corée du Nord et la Corée du Sud, à la suite d'une attaque informatique, les clients de plusieurs banques sud-coréennes ne pouvaient plus retirer d'argent aux distributeurs automatiques.

Face à toutes ces menaces, que faisons-nous ? À la suite du Livre blanc sur la défense et la sécurité nationale de 2008, la France a créé en 2009 l'Agence nationale de sécurité des systèmes d'information, que j'ai l'honneur de diriger. Cette agence, à la fois autorité de sécurité et autorité de défense, rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui dépend lui-même du Premier ministre, a deux missions, l'une de prévention, l'autre de réaction.

Sa mission de prévention consiste à veiller à ce que les infrastructures vitales pour le bon fonctionnement de la nation, publiques ou privées, soient suffisamment protégées et capables de résister à une attaque informatique. L'ANSSI apporte une assistance technique concrète aux opérateurs qui en ont besoin. Ainsi, elle a assisté le ministère des Affaires étrangères pour sécuriser le vote par Internet autorisé lors des dernières législatives pour l'élection des députés représentant les Français de l'étranger. Elle travaille de même avec EDF, avec la SNCF… Un autre volet de sa mission de prévention est de sensibiliser aux risques informatiques et de délivrer des labels à des produits de sécurité ou des prestataires.

L'Agence a pour seconde mission de piloter et de coordonner, sous l'autorité du Premier ministre et du Secrétaire général de la défense et de la sécurité nationale, la réponse en cas d'attaque informatique contre des infrastructures critiques. Elle s'appuie pour cela sur un centre opérationnel actif 24 heures sur 24, sept jours sur sept. Son action peut être comparée à celle des pompiers : des groupes d'intervention sont chargés d'intervenir auprès des administrations ou des grandes entreprises victimes d'attaques, pour les aider à gérer la situation. Il faut savoir que débarrasser les réseaux des pirates n'est pas simple et prend du temps.

Au départ de cent personnes, l'effectif de l'ANSSI atteindra 360 personnes fin 2013, et les recrutements devraient continuer. Que nos effectifs aient ainsi triplé en quatre ans, dans le contexte budgétaire que vous connaissez, dit bien la priorité donnée par le Gouvernement à la sécurité informatique tant la situation est grave.

Quels sont les grands enjeux identifiés lors des travaux préparatoires au Livre blanc et qui devraient trouver leur traduction dans la future loi de programmation militaire ?

Le premier concerne les opérateurs d'infrastructures vitales (OIV). Douze secteurs d'activité d'importance vitale sont identifiés, parmi lesquels la production d'énergie, les transports, les télécommunications, la distribution d'eau, la santé, la finance… – ainsi qu'un peu plus de deux cents opérateurs essentiels à leur bon fonctionnement, dont une bonne moitié est privée. Or, aujourd'hui, la cybersécurité de ces opérateurs ne fait l'objet d'aucune régulation. Alors que l'implantation d'une usine chimique dans notre pays est soumise à une réglementation très stricte, nul ne s'était jusqu'à présent inquiété du fait qu'elle puisse être pilotée par des ordinateurs connectés à Internet sans aucune règle particulière de sécurité, si bien que n'importe quel pirate pourrait en prendre les commandes. L'État ignore leur niveau de sécurité, et leurs opérateurs sont laissés libres en matière de cybersécurité. Nous ne doutons certes pas de leur sérieux mais sous la pression de la concurrence, la recherche de la plus haute sécurité informatique n'est pas nécessairement leur préoccupation première. La volonté du Gouvernement est d'imposer une réglementation en ce domaine.

L'État doit pouvoir édicter des règles que les opérateurs seront tenus de respecter. Je prends un exemple volontairement caricatural, mais qui sera parlant. Il pourrait par exemple être expressément interdit de connecter les commandes d'une centrale nucléaire à Internet. Je vous rassure, dans le cas d'espèce, le problème ne se pose pas.

Il faut également pouvoir imposer à certains opérateurs l'installation de sondes de détection d'attaque informatique, comme il en a été placé aux frontières des réseaux de l'administration. Ces dispositifs de détection relèvent de la souveraineté nationale, au même titre que la cryptographie, et nous devons demeurer autonomes pour leur conception. De même que le concepteur de systèmes cryptographiques est capable d'intercepter et de décoder les systèmes adverses, le concepteur de sondes de détection de cyber-attaques est capable de contourner ces dispositifs de sécurité. Il importe que nous demeurions autonomes dans leur fabrication car ils comportent des informations très sensibles. Si ces informations en fuitant devenaient connues des attaquants, ceux-ci utiliseraient immédiatement d'autres moyens. Il est donc impératif de les garder secrètes.

L'État doit également pouvoir vérifier le niveau de sécurité des opérateurs, qu'il s'en charge lui-même ou qu'il rende obligatoires des audits par des prestataires labellisés. Ces audits auraient pour but de s'assurer que les règles sont bien respectées et de vérifier si les systèmes ne sont pas en danger.

Ensuite, les opérateurs devraient avoir l'obligation de déclarer à l'État les cyber-attaques ayant touché leurs systèmes critiques, entre autres, parce que c'est en analysant certaines attaques qu'on peut en découvrir d'autres. Par ailleurs, si un opérateur dans un secteur donné est attaqué, il y a un fort risque que ses homologues sur le territoire national le soient également. Il est donc essentiel que nous soyons informés en temps réel afin de pouvoir adapter en conséquence nos dispositifs de défense.

Enfin, il faut donner à l'État la capacité, en cas de crise majeure, d'imposer des règles d'action strictes aux opérateurs. Si un incendie menace une voie ferrée ou un axe routier, il est possible de les faire fermer afin de protéger les usagers. Il faudrait pouvoir agir de la même façon en cas de cyber-attaque. Il y va d'ailleurs de la sécurité juridique des décisions prises par les opérateurs pour protéger leurs systèmes, qui peuvent avoir des conséquences sur leur exploitation, et donc financières. Il importe de sécuriser totalement sur

le plan juridique une décision radicale comme l'ordre de déconnecter d'Internet une entreprise.

Ces pistes de travail ne sont pas spécifiques à la France. Des réflexions similaires sont en cours en Allemagne et aux États-Unis. Le projet de directive européenne NIS (*Network and information security*), auquel nous sommes très favorables sur ce point, reprend l'idée d'imposer aux opérateurs des règles minimales. Beaucoup de nos opérateurs critiques opérant également hors du territoire national, il serait utile que les mêmes règles s'appliquent partout. D'une part, cela simplifierait leur tâche ; d'autre part, certains étant présents dans plusieurs pays, leur sécurité repose sur un niveau de protection homogène.

Il importe enfin de sensibiliser à la cybersécurité. En effet, quelles que soient les obligations et les labellisations imposées, si les utilisateurs confient leurs données à n'importe qui et interconnectent leurs systèmes avec n'importe quoi, cela ne servira à rien.

Comme j'aime à le dire, on est aujourd'hui en informatique dans la même situation qu'à la fin du XIX^{e} siècle, lorsque Pasteur découvrait que de nombreuses maladies étaient dues à des microbes et que l'hygiène était donc essentielle pour les combattre. On découvre qu'il faut changer nos comportements et adopter une hygiène informatique. Aujourd'hui, la conception et l'exploitation des systèmes informatiques ne prennent pas assez compte la cybersécurité. Non que les informaticiens, les chefs d'entreprise, les décideurs et les utilisateurs soient inconscients, mais jamais jusqu'à il y a deux ou trois ans, on ne s'en était pas préoccupé. Les ingénieurs ne sont pas formés durant leur cursus à la sécurité informatique, à l'exception de quelques spécialistes, si bien que les systèmes qu'ils conçoivent sont vulnérables à la base. Il est ensuite très difficile de remédier à cette vulnérabilité originelle.

Après une attaque informatique dans une grande entreprise, nous demandons à vérifier le système de gestion des droits d'accès aux messageries afin de vérifier qui pouvait accéder à celle du PDG. On découvre souvent que plusieurs personnes y ont accès : le PDG, sa secrétaire, mais aussi d'autres salariés qui n'ont aucune raison de posséder cet accès. Ce ne sont pas des espions à la solde d'un concurrent, mais tout simplement les pirates informatiques qui utilisent les ordinateurs de ces personnes pour exfiltrer de la messagerie du PDG les informations qui les intéressent. Si, on avait simplement vérifié ces droits d'accès, on se serait rendu compte de l'attaque.

Dans tout système d'information, il existe un mot de passe qui permet d'accéder sans restriction à toutes les données de tous les utilisateurs. La première question que nous posons à un chef d'entreprise est de savoir combien de personnes connaissent ce mot de passe dans son entreprise. Il n'en sait en général rien. Après consultation des directeurs des systèmes d'information, il est arrivé que dans de grandes entreprises, la réponse soit « mille personnes » ! Comment dans ces conditions assurer quelque sécurité que ce soit ? Il suffit qu'une seule de ces mille personnes soit malhonnête ou qu'un pirate s'introduise sur son réseau pour que les données soient détournées. Or, il est possible de ramener le nombre de personnes détenant le mot de passe de mille à dix, sans aucune difficulté et sans aucun coût. C'est là ce que nous appelons l'hygiène informatique. Hélas, ces règles élémentaires ne sont pas enseignées. Les informaticiens ne reçoivent aucune formation en ce domaine, sans parler des chefs d'entreprise et des simples utilisateurs. Que les détenteurs d'une messagerie hébergée à l'étranger ne viennent pas se plaindre si leurs données sont espionnées. Si on

détient des informations sensibles, mieux vaut avoir une adresse de messagerie chez un opérateur français, ou à la Poste. C'est sans doute moins « in », mais au moins, c'est la loi française qui s'applique. Un gros travail de sensibilisation, d'éducation et de formation reste à faire. C'est notre deuxième grand objectif, mais nous savons qu'il faudra du temps avant que les comportements ne changent et que ce n'est pas une loi qui réglera le problème.

M. Jean-Jacques Candelier. Nous vous avons écouté avec le plus grand intérêt et avons beaucoup appris. Le Livre blanc a mis l'accent sur les cyberattaques. Pensez-vous que l'ANSSI aurait besoin de moyens supplémentaires ? J'ai cru comprendre que l'on répondait facilement à vos attentes.

La reconduction par le ministère de la Défense de l'accord-cadre conclu avec Microsoft m'inquiète, surtout après le scandale de la NSA (*National Security Agency*). Cet accord risque de porter atteinte à notre souveraineté nationale. Quel est votre sentiment ?

M. Joaquim Pueyo. Le Livre blanc a fait de la sécurité et de la protection des systèmes d'information et de communication une priorité. Même si cela touche à des domaines pouvant relever de la souveraineté nationale, ne faudrait-il pas renforcer la coopération européenne, dans la mesure où la menace informatique ne connaît pas les frontières et où certains pays n'ont clairement pas les moyens d'une cyberdéfense ? Cette question figure à l'ordre du jour du prochain Conseil européen. La Commission européenne et le Service européen pour l'action extérieure soulignent tous deux l'importance de soutenir le développement des industries européennes de cyberdéfense. Quel est votre sentiment sur la création d'une base industrielle et technologique européenne en matière de cybersécurité ?

M. Patrick Pailloux. Monsieur Candelier, ne demandez jamais à un directeur s'il dispose d'assez de moyens ! Plus sérieusement, le Gouvernement a fait, je le pense, le maximum pour renforcer les moyens de l'ANSSI depuis sa création, et les signaux sont bons pour l'après-2013. L'Agence ne pourrait de toute façon pas grandir beaucoup plus vite car d'une part, il n'est pas si facile d'intégrer de nouveaux personnels en très grand nombre – fin 2013, nos effectifs auront déjà été multipliés par 3,6 depuis 2009 –, d'autre part, nous ne trouverions pas à les recruter. On nous accuse déjà, avec nos collègues de la DGA et des services de renseignement, de « ponctionner » tout ce que notre pays forme d'experts cyber. Il ne serait pas raisonnable de chercher à intégrer plus de 60 à 80 nouvelles personnes par an, ce qui est le rythme actuel hors *turn-over*.

De toute façon, l'ANSSI ne pourra pas répondre seule à tous les besoins, de même qu'il n'y a pas un policier dans chaque logement pour empêcher un cambrioleur de s'y introduire. Il faut pouvoir faire appel à des prestataires capables d'assurer au quotidien la cybersécurité des entreprises et d'intervenir en cas d'attaque. Il est en effet très difficile, même pour de grosses entreprises, de disposer en interne des compétences nécessaires, très pointues. Cela ne serait d'ailleurs pas rentable pour elles. Nous allons labelliser dans les prochains mois les premiers prestataires.

Vous m'interrogez sur l'accord conclu entre le ministère de la Défense et Microsoft. Le piégeage des logiciels n'est plus vraiment un problème, sauf pour des systèmes requérant une très haute sécurité et qui, de toute façon, doivent être isolés pour être parfaitement protégés. N'importe quel système peut être attaqué, une fois repérées ses failles de sécurité, et on trouve tous les jours des failles aussi bien dans les logiciels libres que semi-libres ou

fermés. On peut toujours se demander dans un logiciel libre si elles ont été délibérément introduites par ses concepteurs ou si elles résultent seulement d'un bug de programmation. D'une manière générale, nous préférons plutôt les logiciels libres, parce que leurs codes sources sont accessibles, mais nous savons qu'ils ne sont pas une garantie de sécurité ultime. Le choix entre logiciel libre et logiciel propriétaire dépend avant tout de considérations financières et de gestion. Aucun système, en dehors de systèmes militaires hyper-protégés comme les téléphones ou les chiffreurs secret défense, n'est absolument sûr. Des systèmes d'exploitation tels que Windows ou Linux sont si complexes qu'ils sont par nature vulnérables.

Nous avons bien sûr besoin de coopération européenne, à l'échelle industrielle tout d'abord. Je suis désespéré que l'essentiel des innovations dans les nouveaux usages de l'Internet aient lieu hors de France et que tant de données soient gérées par Facebook et Google. À cet égard, le soutien du Gouvernement à deux opérateurs de *cloud* comme Numergy et Cloudwatt est bienvenu. Nous avons besoin d'acteurs de taille européenne capables de rivaliser avec les grands acteurs américains et chinois. Il importe également, lorsque Bruxelles régule des secteurs comme les télécommunications ou l'énergie, que la question de la cybersécurité soit prise en compte afin d'imposer à tous les opérateurs européens le même niveau de sécurité.

Pour le reste, vous avez raison. Certains pays sont moins bien armés que ne le sont la France, l'Allemagne ou le Royaume-Uni. C'est le rôle de l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information (*European Network Information Security Agency)*, installée à Heraklion, que d'assister les pays qui le souhaitent. Même si sur les cyberattaques, la coopération est conduite entre pays européens de même niveau, il est essentiel que tous coopèrent.

M. Jean-Pierre Fougerat. L'ANSSI a-t-elle des contacts avec tous ses homologues étrangers ? Un réseau a-t-il été créé ?

Étiez-vous au courant de l'espionnage mené par la NSA américaine ? Avez-vous reçu des informations particulières sur ce scandale ?

M. Éduardo Rihan Cypel. Si le nécessaire a été fait dans le Livre blanc pour renforcer les moyens de cybersécurité et de cyberdéfense dans l'appareil d'État et les opérateurs d'importance vitale (OIV), il reste préoccupant que nos entreprises et l'ensemble de la société française ne soient, elles, pas au point en ce domaine. La sécurité informatique relève pour ainsi dire d'une double souveraineté, individuelle et nationale. Il importe pour le citoyen que ses données personnelles soient protégées et pour la Nation que la sécurité nationale soit garantie. Loin de s'opposer, défense des libertés individuelles et défense de la sécurité nationale vont de pair en cette affaire. Comment, pour vous, les deux s'articulent-elles ? Comment les moyens de cybersécurité et de cyberdéfense peuvent-ils permettre de satisfaire ces deux dimensions de la souveraineté ?

M. Patrick Pailloux. Dans nos contacts, nous avons une double stratégie. Tout d'abord, nous cherchons à avoir le carnet d'adresses le plus fourni possible et le plus de contacts possible avec le plus grand nombre de personnes possible – homologues, industriels, *etc.* –, y compris des gens avec lesquels nous ne sommes pas spécialement amis. La situation est très variable selon les pays : il en est dans lesquels nous n'avons pas d'homologue,

d’autres dans lesquels il y en a un ou plusieurs. Dans certains pays, nos homologues sont des universitaires, dans d’autres des services de renseignement. Le second axe de notre stratégie est d’échanger de manière approfondie sur ces questions avec nos grands alliés en ce domaine que sont, sans surprise, le Royaume-Uni et l’Allemagne. Ces échanges sont essentiels dans la mesure où notre capacité de défense repose en grande partie sur la connaissance que nous avons des attaquants.

Non, nous n’étions pas au courant du programme de surveillance américain PRISM. Cela étant, le travail de l’ANSSI est précisément d’imaginer que de telles pratiques existent et de trouver les moyens de s’en protéger. Jusqu’alors, j’étais plutôt critiqué dans le milieu des experts pour mon opposition bien connue au BYOD (*Bring Your Own Device)*, qui fait que des personnes utilisent pour leur travail leurs terminaux personnels, comme un iPhone ou un Androïd. J’ai toujours fait valoir qu’autorisant ces pratiques, une entreprise abandonne une part de souveraineté puisque ce n’est plus elle qui décide de comment elle protège ses données. On me reprochait ce qu’on tenait pour de la ringardise ou de la paranoïa, disait-on. Depuis les révélations de M. Snowden, ces critiques se font beaucoup plus rares… Je suis payé pour être paranoïaque, ai-je l’habitude de dire, et donc pour imaginer que tous les pays espionnent de la sorte, partout et tout le temps, et concevoir les moyens d’y parer. C’est en ce sens que PRISM ne nous a pas surpris.

Vous avez raison, monsieur Rihan Cypel : non seulement protection des données personnelles et protection de la sécurité nationale ne s’opposent pas, mais les deux sujets relèvent de la même problématique. Ce sont les mêmes technologies et les mêmes comportements qui permettent de protéger les chiffreurs secret défense destinés à garantir la souveraineté nationale et les données personnelles des citoyens. À cet égard, je souhaite que projet de carte d’identité électronique aboutisse. En prenant certaines mesures de sécurité et en privilégiant des opérateurs de *cloud* en France et en Europe, relevant donc de la réglementation française ou européenne, on protège tout à la fois la sécurité nationale, nos entreprises et nos citoyens.

M. Philippe Folliot. La visite que nous avions faite à l’ANSSI avec d’autres membres de la commission nous avait permis de mesurer très concrètement les menaces qui pèsent sur les systèmes informatiques.

Il est prévu de faire appel à des prestataires car l’ANSSI ne peut tout faire seule. Le sénateur Bockel proposait dans son rapport sur la cyberdéfense de créer une « cyber réserve » citoyenne. Quels contours cette réserve pourrait-elle prendre ? Comment nos étudiants en informatique, nos informaticiens chevronnés, voire de simples citoyens intéressés par ces questions, pourraient-ils aider en cas de besoin, faisant par là même acte de civisme et de patriotisme ?

On dit au rugby que la meilleure des défenses, c’est l’attaque. N’est-ce pas vrai également en matière de cybersécurité ? Quelle part de ses moyens l’ANSSI consacre-t-elle aux capacités offensives ?

M. Christophe Guilloteau. Nous avons beaucoup travaillé avec mon collègue Eduardo Rihan Cypel sur les aspects cyber lors de l’élaboration du Livre blanc. Celui-ci indique expressément que les administrations devront être sensibilisées aux aspects de sécurité informatique. Le Parlement devra légiférer sur le sujet. Comment est assurée la

coordination entre les différents services chargés de la cybersécurité et de la cyberdéfense dans notre pays ? M. Poupard, spécialiste de ces questions à la DGA, que nous auditionnions la semaine dernière, nous disait qu'il pouvait s'appuyer sur une structure de 250 personnes. Le ministère de la Défense dispose de ses propres moyens. L'armée de l'air par exemple a son propre service de cybersécurité sur la base de Mont-Verdun. Une personne est-elle chargée de la coordination de l'ensemble, comme il existe un coordonnateur national du renseignement ?

M. Patrick Pailloux. Constituer une « cyber-réserve » est une excellente idée, que nous soutenons. Nous participons d'ailleurs à la constitution de cette réserve, avec le ministère de la Défense. Elle aurait deux composantes. Une réserve citoyenne aurait pour mission de trouver des relais d'opinion pour sensibiliser à ces questions, lancer des réflexions, organiser des réunions … Elle est en marche. Une réserve opérationnelle, prévue dans le Livre blanc mais qui n'a pas encore commencé d'être constituée, viserait, elle, à mobiliser des « sachants » auxquels faire appel en cas de problème. Elle permettrait de mobiliser des ressources supplémentaires en cas de besoin et pourrait motiver nos jeunes, à qui la notion de réserve peut sembler datée.

L'ANSSI n'a aucune responsabilité dans le domaine offensif.

Les services chargés de la cybersécurité et de la cyberdéfense ne sont pas nombreux en France, se limitant pour l'essentiel au ministère de la Défense et à l'ANSSI. Le ministère possède ses propres capacités défensives pour protéger les systèmes militaires. Décision a été prise de localiser au même endroit ses équipes de cyberdéfense et celles de l'ANSSI : nous avons emménagé dans un même bâtiment il y a quelques semaines, où se trouve donc regroupé l'essentiel de notre force de frappe en cyberdéfense. La structure chargée de coordonner la cyberdéfense dans notre pays, c'est l'ANSSI, où remonte l'ensemble des informations. Et la coordination s'effectue parfaitement.

Croyez bien que nous n'avons pas trop de ressources. Nous ne sommes pas en mesure d'aider toutes les entreprises victimes d'espionnage informatique et nous sommes obligés d'en inviter certaines à faire appel à des prestataires extérieurs. Le volume des attaques est tel que nous devons en permanence arbitrer pour décider de celles sur lesquelles nous mobiliser en priorité. Là est davantage la difficulté que de savoir comment se coordonner.

M. Philippe Vitel. N'y aurait-il pas intérêt à mutualiser toutes les ressources et à fédérer toutes les structures chargées de cybersécurité et de cyberdéfense ?

Quid de nos relations avec les États-Unis, et surtout la Russie et la Chine ? En avons-nous même en ce domaine avec ces deux derniers pays ?

Quelles relations l'ANSSI entretient-elle avec l'agence de l'OTAN chargée de la cyberdéfense, qui est implantée à Tallinn ?

M. Frédéric Lefebvre. Je suis frappé par l'extrême naïveté des décideurs dans notre pays, économiques et politiques, de droite comme de gauche. Si j'ai bien compris, l'ANSSI intervient essentiellement après qu'une attaque a eu lieu. Aussi bien du côté de la haute administration que des entreprises, il y a aujourd'hui des défaillances dans la capacité à anticiper et prévenir ces attaques que vous avez vous-même, à juste titre, qualifiées de courantes. Que faire pour y remédier ? Le besoin de prévention est criant.

M. Patrick Pailloux. Je ne suis pas certain que l'on pourrait mutualiser beaucoup plus qu'aujourd'hui. Chaque entreprise, chaque administration, chaque organisation doit avoir ses propres capacités de sécurité au niveau élémentaire la concernant. La sécurité de chacun ne peut pas dépendre d'un organisme central qui n'intervient qu'au niveau ultime et pour gérer l'exceptionnel. Le ministère de la Culture ou une banque, au même titre que le ministère de la Défense, doivent disposer de leur propre sécurité. Cependant les enjeux n'étant pas les mêmes, les capacités seront bien sûr différentes.

Avons-nous des relations avec la Russie et la Chine sur ces sujets ? Je puis seulement vous dire que dans le cadre du dialogue stratégique mené avec ces deux pays, les sujets cyber sont évoqués.

L'OTAN possède deux entités chargées du domaine cyber. L'une, en effet implantée à Tallinn, est un centre d'excellence qui se concentre sur les études et la formation. Elle a notamment mené d'intéressants travaux sur le droit de la guerre appliqué au cyberespace. L'autre, le NCIRC (*NATO Computer Incident Response Capability*), située à Mons en Belgique, est un centre opérationnel chargé de piloter la cybersécurité de l'OTAN et, comme son nom l'indique, de réagir aux incidents informatiques. Notre priorité dans ce domaine est que l'OTAN protège suffisamment ses propres réseaux.

Nous avons mis en place aux frontières des réseaux de l'administration des sondes de détection des attaques informatiques. Ce dispositif marche bien, mais il ne constitue qu'une partie de la réponse au problème. Pour le secteur privé, nous cherchons à labelliser les sondes que des prestataires peuvent installer. Au-delà de ces réponses techniques, le besoin le plus criant est de sensibiliser et de former les personnels. L'ANSSI y prend une part importante. Son service de communication, qui emploie aujourd'hui six personnes, publie de nombreux guides de conseils pratiques. Beaucoup de PDG viennent nous dire leurs inquiétudes. À ceux qui nous consultent, nous donnons des clés, nous proposons des méthodes et indiquons les bonnes questions à poser. Nous avons publié un « guide d'hygiène informatique » comportant quarante règles élémentaires comme s'assurer des droits d'accès à la messagerie des dirigeants, limiter le nombre de personnes connaissant le mot de passe donnant accès au cœur du système… Le premier objectif devrait être que ces quarante mesures soient partout respectées – il n'est pas rare que seules une ou deux le soient ! Ce travail de sensibilisation et de formation prendra du temps.

Vous dénoncez, monsieur Lefebvre, l'extrême naïveté des décideurs, mais il y a trois ans, personne, hors des cercles de spécialistes, ne parlait encore de ces sujets. Alors qu'aujourd'hui tous les jours des journalistes demandent à nous rencontrer, il n'y a pas si longtemps, ils ne connaissaient même pas l'existence de l'ANSSI ! On a pendant plus d'un demi-siècle développé l'informatique sans se préoccuper aucunement de sécurité. Nous ferons tout ce qui est possible pour rattraper le retard pris, mais la situation ne pourra pas changer du tout au tout d'un simple claquement de doigts. Cette sensibilisation est du rôle de tous, décideurs politiques, acteurs économiques, médias…

M. Frédéric Lefebvre. Quelles relations l'ANSSI entretient-elle avec le Conseil national du numérique ? Des sondes ont été installées aux frontières des réseaux des administrations, avez-vous dit, mais cela ne suffit pas. *Quid* de la prévention humaine ? Comment sont formés les responsables de notre haute administration ? Lorsqu'un ministre prend ses fonctions, lui demande-t-on, ainsi qu'aux membres de son cabinet, de prendre des

précautions particulières – pour avoir occupé des fonctions ministérielles, je connais la réponse ! Ce qui fait le plus défaut aujourd'hui dans notre pays, c'est la prévention. Comment y remédier ?

M. Patrick Pailloux. Lors de la prise de fonctions du nouveau gouvernement en mai 2012, nous avons adressé un guide de recommandations à l'ensemble des cabinets. Nous intervenons également à l'École nationale de la magistrature, à l'École nationale d'administration… Nous faisons beaucoup mais il faut faire encore davantage. Le fondement de la pédagogie, c'est la répétition. Notre tâche est difficile car il nous faut aller contre la tendance naturelle et contre la mode. Nous luttons contre l'usage professionnel de l'informatique personnelle et l'accoutumance au confort qu'elle crée. La sécurité, c'est contraignant, moins commode… Des appareils plus sécurisés ne sont bien entendu pas aussi ergonomiques et conviviaux qu'une messagerie Gmail sur un iPhone ou un Galaxy S 4 !

J'oubliais de dire que l'ANSSI a un centre de formation, le CFSSI, où sont toute l'année dispensées des formations à l'intention des agents de l'administration de tous niveaux, allant d'une journée de sensibilisation à une formation spécialisée d'une année entière.

M. Jean-Yves Le Déaut. Où trouvez-vous les experts dont vous avez besoin ? Il est patent que notre pays ne forme pas assez de spécialistes en cybersécurité.

Pour avoir travaillé sur ces sujets, j'ai l'impression qu'il n'existe pas assez de liens entre les domaines militaire, civil et universitaire. Comment pourrait-on renforcer ces liens ? Les universités travaillant dans ces domaines ou les organismes de recherche comme l'INRIA sont-ils en relation étroite avec la DGA ? Ainsi le laboratoire de haute sécurité informatique, situé au sein du centre INRIA Nancy Grand Est, est-il en lien suffisant avec le centre DGA-MI (Direction générale de l'armement – maîtrise de l'information) de Bruz en Ille-et-Vilaine ?

L'offensive n'est pas de la responsabilité de l'ANSSI, dites-vous. Je pense, pour ma part, qu'il faudrait réglementer ce domaine et donner la possibilité de travailler, y compris dans les laboratoires universitaires, sur les capacités offensives. Je n'ignore pas que cela n'aide pas nécessairement à se protéger mais cela permet au moins de mieux identifier les failles de sécurité et de mieux connaître, au moins sur le plan théorique, les systèmes.

La cryptographie a toujours relevé de la souveraineté nationale. Il a été décidé que la géolocalisation en relèverait aussi puisqu'on souhaite se doter d'un système alternatif au GPS. Mais lorsque nous achetons des drones sur lesquels nous n'aurons jamais accès aux codes sources, n'abandonnons-nous pas une part de notre souveraineté ? De même, n'est-ce pas abandonner de notre souveraineté que de laisser la gouvernance mondiale d'Internet aux mains d'un seul pays ? Ne pourrions-nous pas être plus offensifs sur ce point ?

M. Yves Fromion. Ne confondons pas la cyberdéfense et ce qui relève simplement d'écoutes sur Internet, comme dans l'affaire Snowden ! Les deux peuvent se recouvrir partiellement mais il ne faut pas mélanger les choses.

Vous avez évoqué la prévention et la formation nécessaires. A-t-on commencé de développer dans les universités et les écoles – je pense à l'ENSI de Bourges dans ma circonscription, spécialisée notamment en sécurité informatique – des modules de formation, de façon que la jeune génération d'étudiants porte la préoccupation de la cybersécurité comme dans ses gènes ?

M. Patrick Pailloux. Il n'existe pas aujourd'hui de modules obligatoires de cybersécurité dans les cursus d'ingénieur. Faut-il en imposer ? Il faut en tout cas convaincre les écoles et les universités de la nécessité d'en prévoir systématiquement. Il n'est pas admissible qu'un ingénieur informaticien termine aujourd'hui ses études sans qu'on lui ait enseigné les règles élémentaires de l'hygiène informatique. On n'attend pas la fin de leurs études pour apprendre à une infirmière ou un médecin qu'il faut se laver les mains et stériliser les matériels !

Où trouvons-nous les spécialistes formés à la cybersécurité dont nous avons besoin ? Essentiellement dans les écoles, mais il y a quelques autodidactes. Une analyse conduite avec nos partenaires industriels qui recrutent eux aussi beaucoup est que nous formons un tiers seulement des experts qui seraient nécessaires. D'où le soutien que nous apportons à toutes les initiatives de cursus en cybersécurité.

L'ANSSI n'a pas de capacités offensives car ce n'est pas sa mission. Il est vrai, comme vous l'avez dit, que l'offensif, y compris le *reverse*, peut servir à comprendre les attaques. On ne peut toutefois laisser toutes les actions se développer partout car elles sont dangereuses. Il faut pouvoir les contrôler. Cela ne veut pas dire que l'on ne puisse pas faire davantage qu'aujourd'hui.

Lorsque j'ai parlé de souveraineté, je ne visais que le champ de la cybersécurité. Il en est bien d'autres, mais bien entendu je plaide pour mon domaine, qui est en quelque sorte la « souveraineté de la souveraineté ». Si nous ne sommes pas capables de protéger nos propres données, le reste ne sert à rien. À quoi servirait de concevoir entièrement par nous-mêmes des systèmes de défense placés sous notre contrôle exclusif si nous sommes impuissants par ailleurs à assurer leur protection ? Reste à savoir contre qui se protéger, et donc analyser les risques quand on achète un équipement.

On en est encore très loin d'un traité international pour le cyberespace, d'autant que les positions de départ divergent fortement entre les pays, certains souhaitant qu'on contrôle les contenus, d'autres les contenants, certains privilégiant la liberté, d'autres le contrôle. Des discussions ont commencé aux Nations unies qui ont donné de premiers résultats, mais ce n'est qu'un tout début.

Aucun pays ne contrôle aujourd'hui Internet. Pendant longtemps, l'essentiel du trafic mondial d'Internet transitait par les États-Unis. Ce temps est révolu. Ce sont plutôt de grandes sociétés privées à la pointe de l'innovation, dont il est vrai que beaucoup sont américaines, qui aujourd'hui centralisent et maîtrisent les données qui circulent sur Internet. Le problème d'Internet n'est pas qu'il soit gouverné par un État mais bien plutôt qu'il n'ait ni gouvernance ni régulation – ce qui explique d'ailleurs en partie sans doute son succès. Ainsi, bien qu'une grande partie des communications internationales soient effectuées par le biais de Skype, qui permet de communiquer gratuitement d'ordinateur à ordinateur, ce logiciel échappe à toute réglementation internationale du secteur des télécommunications. Internet est un domaine fondamentalement non régulé où ce sont les meilleures idées économiques qui l'emportent. Skype a marché parce que c'était une bonne idée.

M. Philippe Nauche, président. Monsieur, nous vous remercions. Vos propos éclaireront très utilement la réflexion de notre commission.

La séance est levée à dix-neuf heures.

*

* *

Membres présents ou excusés

Présents. - M. Nicolas Bays, M. Jean-Jacques Candelier, Mme Nathalie Chabanne, M. Guy Chambefort, M. Jean-Louis Costes, M. Philippe Folliot, M. Jean-Pierre Fougerat, M. Yves Fromion, Mme Geneviève Gosselin-Fleury, M. Christophe Guilloteau, M. Jean-Yves Le Déaut, M. Frédéric Lefebvre, M. Christophe Léonard, M. Philippe Meunier, M. Philippe Nauche, Mme Émilienne Poumirol, M. Joaquim Pueyo, M. Eduardo Rihan Cypel, M. Gwendal Rouillard, M. Philippe Vitel

Excusés. - M. Ibrahim Aboubacar, M. Olivier Audibert Troin, M. Claude Bartolone, M. Philippe Briand, M. Guy Delcourt, Mme Edith Gueugneau, M. Éric Jalton, M. Bruno Le Roux, M. Maurice Leroy, M. Alain Marty, M. Jacques Moignard, M. François de Rugy, M. Jean-Michel Villaumé