ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

# Compte rendu

## Office parlementaire d'évaluation des choix scientifiques et technologiques

Examen du rapport d'information de Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur, premier vice-président de l'OPECST, sur le risque numérique

Mercredi 17 décembre 2014

Séance de 16 heures

Compte rendu n° 59

SESSION ORDINAIRE DE **2014-2015**

**Présidence de M. Jean-Yves Le Déaut, député, *Président***

ASSEMBLÉE NATIONALE

**Office parlementaire d'évaluation des choix scientifiques et technologiques**

**Mercredi 17 décembre 2014**

**Présidence de M. Jean-Yves Le Déaut, député, président**

*La séance est ouverte à 16 h 15*

**– Examen du rapport d'information de Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur, premier vice-président de l'OPECST, sur le risque numérique**

**M. Jean-Yves Le Déaut, député, président de l'OPECST**. – Nous allons entendre la présentation du projet de rapport de Mme Anne-Yvonne Le Dain, députée, et de M. Bruno Sido, sénateur, premier vice-président de l'OPECST, sur le risque numérique. Selon une méthode maintenant éprouvée, nous avons mis le projet de rapport en consultation. Cette consultation est organisée sur place dans chaque assemblée. Il est simplement demandé aux membres de l'Office de prévenir de leur arrivée pour éviter de mobiliser le secrétariat pendant des journées entières.

Je vous rappelle que la saisine relative au risque numérique a été effectuée par la commission des affaires économiques du Sénat le 26 juin 2013 et que nous avions organisé quelques mois auparavant, le 21 février 2013, une audition publique en lien avec les deux commissions de la défense de l'Assemblée nationale et du Sénat. Le sous-titre de cette audition se présentait déjà comme une piste de solution : « *Le risque numérique : en prendre conscience pour mieux le maîtriser* » et était déjà apparue la nécessité d'observer les règles d'hygiène informatique pour utiliser les outils numériques. En effet, la sécurité n'est pas seulement une affaire de technique ou de protection mais appelle aussi à la vigilance permanente à tous les niveaux.

Le présent projet de rapport entre dans le détail de la technologie pour mieux faire ressortir les pratiques possibles. Parmi celles-ci, je mentionnerai notamment le chiffrage par clé publique/clé privée qui consiste à conserver par devers soi la clé privée, indispensable au décodage, tandis que l'on donne à toute personne qui envoie un message une clé publique permettant de chiffrer son message.

Le projet de rapport contient des recommandations très nombreuses, près de cent cinquante. Nous reviendrons sur leur contenu après leur présentation. Il me semble, après en avoir parlé avec les rapporteurs, qu'un travail de synthèse et de regroupement de certaines de ces recommandations pourrait être réalisé. Certaines appellent des modifications de nature législative ou règlementaire ; d'autres sont plus techniques. On gagnerait à faire ressortir des recommandations principales, qui s'attachent à essayer de redéfinir les principes de la société numérique. Vous avez vous-même prévu une hiérarchisation pour mettre en valeur certaines recommandations. J'y ai moi-même travaillé ce matin.

Après la projection du petit film prévue en introduction et la présentation par les rapporteurs, je souhaiterais qu'on puisse voir comment on pourrait arriver, sur un certain nombre de points, à modifier un peu le projet de rapport.

*La présentation du jeu « Keep On Eye » élaboré par le CIGREF est projetée.*

**M. Bruno Sido, sénateur, premier vice-président, rapporteur**. – Mme Anne-Yvonne Le Dain et moi-même avons aujourd'hui le plaisir de vous présenter le projet de rapport sur le risque numérique dont vous nous avez confié l'élaboration.

C'est à partir d'une saisine de la commission des Affaires économiques du Sénat que nous avons entrepris une étude de faisabilité adoptée le 16 avril 2014.

Cette saisine faisait elle-même suite à une journée d'auditions publiques organisées conjointement par l'OPECST et la commission des Affaires étrangères et de la Défense du Sénat au mois de février 2013. Ce jour-là, l'audition publique avait été scindée en deux parties, l'une relative au risque numérique militaire et l'autre au risque numérique civil.

Nous comptions donc réaliser notre rapport en approfondissant la question du risque numérique civil mais il nous est rapidement apparu que, en matière de risque numérique, la distinction entre le civil et le militaire était artificielle compte tenu justement de la nature du numérique qui est présent partout.

Au terme d'une centaine d'auditions comprenant trois journées d'auditions publiques et des déplacements à Bruxelles et en province, notamment pour visiter le centre de haute sécurité de la Direction générale pour l'armement et le laboratoire de haute sécurité de l'INRIA, vos rapporteurs ont établi une douzaine de constats sur la situation de la sécurité numérique et procédé à des choix pour mener à bien leur étude.

Au début de celle-ci, nous avons pris soin de rencontrer le président de la commission des Affaires économiques du Sénat, M. Daniel Raoul, aujourd'hui de retour à l'OPECST ce dont nous nous réjouissons.

Nous lui avons indiqué que nous centrerions notre réflexion sur les opérateurs d'importance vitale, c'est-à-dire les entreprises dont le fonctionnement ne doit en aucun cas être interrompu, notamment du fait d'une défaillance de leur système d'information numérique.

Ces entreprises sont d'ailleurs soumises à des directives nationales de sécurité (DNS) qui leur imposent des obligations extrêmement précises. La loi de programmation militaire de 2013 les a renforcées.

L'angle d'attaque pour aborder l'étude à partir des opérateurs d'importance vitale s'est révélé intéressant pour le raisonnement mais conduisait aussitôt à replacer l'ensemble des activités desdits opérateurs dans la chaîne de sécurité qu'ils constituent avec leurs fournisseurs, leurs sous-traitants, leurs clients et leurs personnels.

En outre, pour être tout à fait complet, au moment où le Gouvernement annonçait un ambitieux projet de loi sur le numérique, il n'a cependant pas attendu le dépôt de celui-ci pour prendre, d'une part, comme déjà indiqué, dans la loi de programmation militaire, en 2013, des initiatives relatives justement aux opérateurs d'importance vitale et, d'autre part, pour élaborer, au cours de l'été 2014, des mesures relatives à la sécurité numérique concernant les administrations.

Ce qui montre que le Gouvernement comme nous-mêmes avons été conduits à effectuer des analyses rigoureuses sur les différents secteurs pour finalement constater que tout se recoupe et que la sécurité numérique, voire la sécurité tout court, ne peuvent être assurées qu'à partir de mesures reliées entre elles.

Par quelque bout que l'on considère la question, il est impossible de ne pas voir dans les ramifications du numérique le système nerveux de la société et des individus qui la composent, d'où l'impossibilité de scinder artificiellement les préoccupations de sécurité en divers segments d'études.

C'est bien ce qu'ont vu, en premier, les attaquants des systèmes numériques. À l'heure où notre pays se trouve placé sous les dispositions du plan Vigipirate à un très haut degré – dit « écarlate » –, le thème d'étude de l'OPECST ne peut qu'être au cœur des préoccupations de tous les parlementaires.

Pour relancer ce défi, depuis quelques années, des dispositifs ingénieux ont été imaginés et des moyens réels en hommes et en moyens ont été accordés. Par exemple, en 2009, l'Agence nationale de sécurité des systèmes d'informations (ANSSI) a été créée.

Mais je dois préciser, dès l'abord, que des dispositifs étaient déjà en place et que, maintenant, ce n'est pas en accordant toujours davantage de compétences à l'ANSSI ni en portant ses effectifs de trois cents à mille ou à trois mille – seuils qui ne sont d'ailleurs nullement envisagés –, qu'on résoudrait les questions posées par les failles de la sécurité numérique et qu'on parerait aux attaques dont elle est l'objet.

En effet, cette question transversale suppose l'acquisition, par l'ensemble de la société, d'une culture du numérique et d'une éducation initiale et continue à la hauteur des services rendus par cette technique, en dépit des fragilités qu'elle recèle.

Depuis le début de mon propos et surtout à la suite de la vidéo que vous venez de regarder, vous vous demandez peut-être si vos rapporteurs n'ont pas cédé à quelque alarmisme. Je vous rassurerai en disant que nous avons d'abord souhaité démontrer, dans une analyse que l'on a voulu extrêmement fouillée, le mécanisme de transmission des messages et les fragilités, souvent de conception, des matériels, des réseaux, des services et des diverses applications numériques.

À un moment donné, il nous est apparu que les imperfections constatées peuvent constituer également des chances et c'est cet aspect que Mme Anne-Yvonne Le Dain va maintenant développer pour vous montrer la face optimiste de l'analyse de vos rapporteurs.

Mme Anne-Yvonne Le Dain, députée, rapporteur. – Au fur et à mesure des auditions, une idée m'a de plus en plus préoccupée : comment tirer parti d'une difficulté, d'une inquiétude, d'un mal éventuel et, en l'occurrence, en matière d'insécurité numérique, comment faire de l'économie avec du droit ? À partir du droit national, du droit européen et même du droit international.

Il se trouve que la France possède de nombreux atouts en ce domaine, tant en matière de logiciels et de matériels qu'en matière de connaissances, notamment grâce à l'École française de mathématiques qui a été à l'origine d'une grande tradition en matière de cryptologie et de cryptographie. S'y ajoutent les ressources des universités, des centres de recherche de la Direction générale de l'armement, du CNRS ou de l'INRIA, pour ne citer

qu'eux. Elles devraient permettre de conforter les entreprises œuvrant en ces domaines et, surtout, de faire en sorte que de nouvelles initiatives puissent naître sans être récupérées aussitôt par nos concurrents principaux, à savoir les États-Unis d'Amérique au moment où l'Union européenne est en train de négocier un accord commercial transatlantique.

Dans le monde du numérique, beaucoup de dispositifs sont en autorégulation alors que, au niveau national comme au niveau international les enjeux économiques sont considérables. Les entreprises nord-américaines, les *GAFA (Google, Apple, Facebook et Amazon*) agissent à ce niveau et sont extrêmement présentes, y compris à Bruxelles où se bâtit le cadre de l'économie numérique du XXI$^{ème}$ siècle. L'enjeu est colossal. Le numérique touche tout, dans la vie personnelle comme dans la vie professionnelle de chacun, les personnes physiques comme les personnes morales.

Pour mettre en valeur les atouts français, il faut se débarrasser de préjugés et d'attitudes routinières. Par exemple, les préjugés associés à l'image des *hackers* qui peuvent également être employés fort utilement pour devenir, non pas des pirates, mais des corsaires au service des institutions qui les emploient.

On voit bien qu'il s'agit actuellement d'un enjeu absolument stratégique et c'est ce qui a motivé la rédaction de ce rapport.

À ce stade de notre travail, nous avons auditionné beaucoup de monde et accompli beaucoup de travail avec le président Bruno Sido, et je pense que les cent quarante recommandations qui vous sont proposées sont tout à fait importantes, mais qu'il serait pertinent, sur la base du document, qui représente un énorme travail, dont je remercie les administrateurs, de consacrer encore un peu de temps pour réécrire, reformuler, revoir la manière dont les choses sont dites ;pour communiquer de manière plus efficace dans un contexte où, en ce moment, entre l'Union européenne et les États-Unis d'Amérique, et dans les relations internationales en général, les enjeux dans ce domaine sont considérables.

Il serait souhaitable de prendre encore deux à trois semaines après les vacances pour revoir un certain nombre de finalités, pour reformuler, reclasser et donner des priorités en ce domaine. L'enjeu est essentiel ; on a pu le mesurer en entendant énormément de monde, en se posant la question de la protection des données individuelles et personnelles dont les volumes ont explosé.

Au moment de la décision de lancer la présente étude, l'affaire Snowden n'était pas encore sur la table et le piratage du portable de la chancelière allemande n'était pas encore connu. Nous avions anticipé. Maintenant, l'environnement national et international a encore évolué et il serait essentiel de prendre un peu de temps pour reformuler un certain nombre de choses. Je vous remercie.

**M. Jean-Yves Le Déaut, député. –** Je souhaiterais d'abord dire que, y compris les schémas que je trouve très, très bien, il y a là un matériau de fond qui est bon. Vous demandez un peu de temps car j'ai cru comprendre que vous aviez été « charrette » sur la fin. Je voudrais remercier l'administrateur et l'expert qui l'a assisté, du travail qui a été fait.

J'ai vu le rapport ce matin et n'ai eu qu'un peu de temps pour y travailler. Je pense d'abord, à propos du projet de recommandations, que l'on peut arriver à une très bonne étude de l'Office en ordonnant les cent quarante ou cent cinquante recommandations qui sont là

pour mettre en valeur des schémas que vous avez élaborés et qui expliquent parfaitement la problématique.

Le premier point que je voudrais signaler c'est que la partie introductive du projet de recommandations intègre un rappel du guide de l'ANSSI. Or, notre but, à l'Assemblée nationale comme au Sénat, n'est pas de reprendre des dispositions qui existent déjà mais de sélectionner, dans les recommandations de l'ANSSI, les points sur lesquels il y aurait moyen de faire évoluer les choses.

J'ai donc pris la responsabilité de faire une proposition de rédaction pour les recommandations que je vous transmettrai tout à l'heure. J'ai ordonné autour de six chapitres les propositions : le premier chapitre s'intitulerait « *Développer une culture du numérique autour de la sphère politique et administrative* ». Le deuxième point, que vous avez très bien traité à mon avis, concernerait le risque numérique ; cela est plutôt bien et je reprends vos recommandations. Le troisième point consisterait à faire du risque numérique une grande cause nationale dans l'éducation et la formation et tout ce que vous proposez apparaît sous ce chapitre. Le quatrième chapitre serait « *Renforcer les moyens de la formation universitaire et de la recherche en matière de cyber-sécurité* » ; c'est le point le moins abordé dans les recommandations, mais c'est un débat dans lequel je suis déjà intervenu pour dire que, à côté du pôle militaire de défense situé dans l'ouest de la France, il existe un autre pôle de cyber-sécurité civile, dans une autre région, consacré à des thèmes de recherche qui pourraient le situer à un niveau européen. Cinquièmement, il s'agit de mieux protéger les entreprises et c'est là l'essentiel du rapport. Il serait plus efficace pour aider les entreprises d'indiquer quatre ou cinq grands points d'évolution possible de la loi.

Toutes les autres propositions seraient alors placées en annexe sous la forme d'une ébauche d'un guide de cyber-sécurité à destination des entreprises. Toutes les dispositions pratiques pourraient également être hiérarchisées. Enfin, il faudrait insérer la stratégie nationale dans une stratégie européenne et, sur certains points, j'aimerais que les rapporteurs nous indiquent comment ils voient le débat citoyen dans le domaine du risque informatique ; comment ils appréhendent la possibilité d'imposer le respect sur Internet de la présomption d'innocence, celle du contradictoire et des prescriptions. Il serait souhaitable aussi d'interdire la captation des données à distance et, pour cela, de déterminer ce qui est législatif dans ces recommandations.

Il faudrait également encourager le développement d'acteurs de confiance, ce qui pourrait entraîner des retombées économiques. Très souvent, dans vos conclusions finales, vous attirez l'attention sur ces retombées économiques possibles et cela mériterait des précisions. Enfin, il y a d'autres points qui devraient sans doute être déplacés d'un chapitre à un autre si ma proposition en six points était adoptée.

Ce matin, je me suis livré à un exercice de nouvel ordonnancement des recommandations. Vous avez mes notes et il est possible d'agencer cela autrement tout en améliorant la formulation des idées sachant que le fond de ce texte est excellent et qu'une amélioration formelle serait, à mon avis, de nature à faire passer les bons messages qui sont dans ce rapport.

Et, ce, d'autant plus que les rapporteurs, même s'ils ne l'ont pas dit, n'ont pas eu suffisamment de temps pour étudier ce projet de rapport en dépit de l'existence d'un pré-rapport. Cela a été trop « charrette » de finaliser complètement ce projet pour la fin de l'année. Donc, si les deux rapporteurs le demandent, cette réunion de l'Office parlementaire

pourrait constituer une réunion de travail en vue de l'élaboration d'un nouveau texte à valider et à examiner rapidement par la suite puisque les rapporteurs ont déjà en partie commencé leur présentation.

Il n'y a aucun problème à procéder de la sorte car les thèmes que vous avez abordés sont des thèmes majeurs.

Peut-être serait-il souhaitable d'insister sur la partie recherche et enseignement supérieur et j'aimerais que, dans le corps du texte, vous rajoutiez un point – qui figure dans mon avis budgétaire sur la cyberdéfense –, pour souligner qu'il risque de manquer de personnes formées à la cyberdéfense dans les prochaines années ; si vous en étiez d'accord, peut-être serait-il souhaitable de mettre ce point en exergue de manière plus évidente ?

**M. Bruno Sido.** – On est toujours pressé par le temps et il est toujours possible de revisiter et de réordonner ce projet de rapport, sans changer le fond puisque c'est le résultat de nos investigations. Mais, sur la forme, il est toujours possible de placer des éléments en annexe. La version définitive vous sera soumise avant l'examen par l'Office pour vous donner le temps de bien apprécier la forme définitive.

**Mme Anne-Yvonne Le Dain. –** C'est un travail colossal. Le président Bruno Sido, moi-même et l'administrateur avons consacré un temps colossal aux auditions dont trois auditions publiques incluant des table rondes plus confidentielles et cela a permis d'embrasser tout le champ de ce sujet stratégique ; il était temps de le faire. Cela représente un joli travail sous réserve d'une remise en forme finale pour améliorer la visibilité de ce rapport pour le rendre plus efficace aux yeux du grand public comme des média ; c'est aussi simple que cela.

**Mme Marie-Christine Blandin, sénatrice. –** Je n'ai pas grand-chose à dire à part mon admiration pour la densité de ce qu'on trouve dans ce rapport : c'est une bible. Peut-être y a-t-il une ergonomie à développer pour mieux accéder au contenu, mais c'est vraiment très riche et très bien.

Pour ma part, je n'étais pas sur le champ exclusif de l'entreprise car la commission de la culture du Sénat avait travaillé sur des thèmes qui sont aux frontières du sujet de ce rapport. Par exemple, à la page 41, vous parlez de la régulation de l'échange entre les personnes physiques, puis après, on passe au virtuel. Nous avions travaillé sur le virtuel pour lequel il apparaît que, si les gens ne s'adressent pas des signes préalables, un sourire préalable, rapidement un propos peut être à l'origine de polémiques. C'est pourquoi, les discussions sur Internet, par exemple de syndicats ou de partis politiques, s'enveniment avec méchanceté et des modérateurs ont donc été mis en place. Le numérique fait apparaître de nouveaux acteurs et de nouveaux pouvoirs car les modérateurs sont des gens de pouvoir. Cela a également de l'importance dans l'entreprise parce que le modérateur prend le pouvoir alors que personne ne s'en aperçoit. Il filtre les débats avec ses convictions.

Ensuite, tout acte public pris par le passé a donné lieu à des archives papiers ; elles se trouvent à la Bibliothèque nationale et sont consultables dans les archives départementales, etc. Maintenant, le numérique donne le pouvoir à celui qui émet des documents de les détruire. J'en donnerai quelques exemples : une des académies – je ne sais plus si c'est celle des sciences, celle de médecine ou celle des technologies – a fait disparaître un rapport sur l'amiante datant d'une époque où elle estimait que cette matière n'était pas dangereuse, ce qui est tout de même gênant [*Des signataires issus de l'INSERM se sont désolidarisés* a posteriori *du rapport de l'Académie de Médecine : « Amiante et protection de la population exposée à*

*l'inhalation de fibres d'amiante dans les bâtiments publics et privés », Bulletin de l'Académie Nationale de Médecine ; Tome 180 n°4 – séances des 16, 23, 30 avril 1996, page 887*]. Le numérique permet très facilement ce genre d'opérations de disparition.

Quant à l'AFSSAPS – on avait travaillé là-dessus avec M. Jean-Pierre Door –, au moment de la pandémie grippale, il a fallu vacciner tout le monde donc, en catastrophe. Sanofi, GSK et Roche ont mis au point des vaccins comprenant des sels d'aluminium. Moi, je me souvenais qu'une page de l'AFSSAPS disait que les sels d'aluminium posaient problème, qu'il fallait les interdire aux enfants de moins de deux ans et que, à terme, il n'y aurait plus de vaccins de ce type. J'ai donc recherché cette page mais ne l'ai pas trouvée. Je pouvais avoir rêvé sauf qu'une étudiante en médecine qui avait fait sa thèse sur les vaccinations avait pris une copie d'écran de cette page et c'est donc ainsi que je l'ai retrouvée.

Je ne parle pas du fond, mais le numérique donne le pouvoir de détruire des archives publiques et une réflexion démocratique doit être conduite là-dessus, car cela pose tout de même un problème.

Je continue, toujours un peu en marge de votre rapport, à propos de préoccupations relatives aux libertés individuelles. Je ne suis pas sur *Facebook*. J'ai reçu de nombreuses invitations d'amis qui y sont et, la dernière fois, j'ai reçu une invitation de personnes souhaitant m'inviter avec la liste de tous mes amis, de mon beau-fils, de mon ancienne collaboratrice etc. Cela fait froid dans le dos car, si l'on repense aux réseaux de résistance, on se dit que si, aujourd'hui, nous nous trouvions dans la même situation, n'importe quelle police fasciste, en appuyant sur un bouton, pourrait obtenir tous les lieux où vous pouvez vous cacher, toutes vos relations... Je ne suis pas sur le réseau, et, pourtant, les gens qui me mentionnent sur le réseau y développent en creux l'imagerie de mes amis et, cela, c'est un problème de liberté.

Certaines de vos recommandations sont relatives à l'éducation et à l'enseignement supérieur. Je souhaiterais alerter sur la mauvaise formation des étudiants au numérique et sur le plagiat. En effet, de plus en plus de thèses sont plagiées dans les universités ; cela constitue un vrai problème au point que, lors de son audition au Sénat, M. André Syrota, de l'Institut national de la santé et de la recherche médicale (Inserm) et de l'Alliance pour les sciences de la vie et de la santé (Aviesan), nous a alertés sur le fait que 40 % des publications, dans *Nature*, de découvertes, d'innovations etc. n'étaient pas reproductibles parce que le travail n'est pas fait de première main. Cela pose problème.

Vous parlez de la compétitivité des entreprises. La commission de la culture du Sénat a travaillé sur les entreprises de presse, qui gagnent leur argent sur la publicité, mais, depuis que *Google* les référence et se place entre les publicitaires et les agences de presse, c'est *Google* qui ramasse l'argent.

La Belgique a souhaité élaborer un texte pour empêcher cela, mais *Google* a débranché toutes les entreprises de presse belges du référencement. Tout récemment, *Google plus* vient de débrancher l'Espagne qui préparait un nouveau texte de loi dans ce domaine. Ce qui donne une idée du pouvoir de ces monopoles. Dans votre rapport, vous parlez beaucoup du risque des monopoles.

Ensuite, dans un passage, vous évoquez la mentalité des *hackers*. Avec *Le Monde diplomatique*, nous avions réuni les *Anonymous*. C'était impressionnant, car ils nous ont expliqué comment ils avaient aidé la démocratie en Égypte pendant la répression ; de même

en Tunisie. Tous les journalistes du *Monde* souriaient et trouvaient ces jeunes gens formidables mais, par derrière, ceux-ci nous ont précisé qu'ils n'avaient qu'une ligne, celle de la circulation de l'information : si un chef d'État fasciste voulait susciter l'adhésion de jeunes, et au moyen d'un message à la jeunesse, et qu'un autre État souhaite l'empêcher, les *Anonymous* feraient en sorte que ce message parvienne jusqu'à elle. Ils entendent être inodores et incolores ; leur philosophie, c'est la sacralisation du message.

Merci donc pour votre rapport.

À propos du coût éventuel de la sécurité numérique sur la compétitivité des entreprises, je souhaiterais peut-être un petit ajout pour évoquer l'engrenage de l'obsolescence et des coûts induits parce que je vois que, au sein de l'éducation nationale, dans les établissements scolaires, certains commencent à « se faire des cheveux blancs » à cause des achats de logiciels, du renouvellement de matériel, *etc*. Pour cette raison là aussi, nous sommes incités de nous trouver face à des monopoles, pour faire jouer la concurrence et obtenir des prix raisonnables ; sinon cela va nous coûter toujours plus cher.

Par ailleurs, mais c'est peut-être évoqué dans le projet de rapport que je n'ai pu lire intégralement, qu'en est-il de la vulnérabilité physique des centres de stockage de données ?

J'ai conscience que mes commentaires sont parfois un peu aux limites du thème de la sécurité numérique des entreprises.

**M. Bruno Sido.** – Nous nous sommes aperçus, quasiment dès le départ, que le champ d'investigation était tellement vaste que, au-delà des généralités, nous nous sommes dit qu'il serait intéressant de traiter plus particulièrement, à titre d'exemple, du secteur de l'énergie et du secteur des télécommunications, deux secteurs parmi tant d'autres. Et nous ne pouvons même pas dire si les problèmes soulevés dans ces deux secteurs sont les mêmes que ceux d'autres secteurs – bancaire, administratif, universitaire… –, cela reste à examiner.

Les remarques faites par Mme Marie-Christine Blandin sont tout à fait pertinentes et intéressantes. Heureusement pour les thèses, le plagiat était devenu tellement répandu qu'il y a maintenant des logiciels pour le détecter.

**Mme Anne-Yvonne Le Dain. –** Je vous remercie pour cet élargissement des perspectives. Le champ du numérique est gigantesque, car le numérique est vraiment partout. Il est impossible de le traiter dans son ensemble. Nous avons souhaité indiquer la manière dont on pourrait se protéger des risques grâce à des guides de bonnes pratiques, même si cela apparaît très difficile du fait, notamment, de l'existence de portes dérobées dans les matériels.

Nous n'avons pas seulement à subir le numérique, mais aussi à nous en saisir pour en faire une opportunité économique, de manière à se protéger tout en se développant, d'autant qu'il s'agit d'un enjeu mondial.

**M. Bruno Sido.** – Nous nous sommes aperçus, sans entrer forcément dans la technique, que l'application de quelques principes de bon sens permettait de se prémunir pour l'essentiel de l'insécurité numérique. La première chose, c'est déjà d'en avoir conscience. Quand on pense que des patrons se rendent en Chine avec leur ordinateur et leurs tableaux de calcul, travaillent avec ces outils sur place et s'aperçoivent à leur tour que, finalement, s'ils n'ont pas remporté le marché, c'est parce qu'au passage de la frontière, on avait capturé toutes

leurs données, y compris celles de leurs téléphones. Il vaut mieux se rendre en Chine avec un petit téléphone neuf que l'on jette au retour.

La deuxième chose c'est l'hygiène informatique : il faut savoir qu'il vaut mieux ne pas ramasser de clés *USB*, puis s'en servir ; en fait, c'est comme pour sa brosse à dents, il vaut mieux ne jamais la prêter.

Enfin, l'administration s'est bien adaptée depuis un certain temps, et c'était d'ailleurs extrêmement important. De leur côté, les opérateurs d'importance vitale (OIV) donnent l'exemple.

On nous a dit, à propos des feux de signalisation informatisés aux carrefours, ce que tous les responsables de la préfecture de police de Paris savent : en cas de panne du système informatique de ces feux, il y aurait des blessés, voire des morts ; car, en moins de deux heures, les gens en viendraient aux mains si tout s'arrêtait.

L'ANSSI a déjà été reformatée, mais elle a du mal à embaucher, quoiqu'elle n'hésite pas à faire appel aussi à des *hackers* repentis. D'ailleurs, certains sont-ils peut-être devenus *hackers* pour se faire remarquer à cette fin ? La direction générale pour l'armement travaille également à la sécurité numérique vingt-quatre heures sur vingt-quatre et, ce matin, j'assistais à une réunion de la Commission supérieure du service public des postes et des communications électroniques au cours de laquelle le Premier ministre a dit que le numérique et sa sécurité constituaient une priorité, qu'il ne fallait pas que le numérique flanche sinon plus rien ne se passerait aujourd'hui. Tout le monde a bien pris conscience de cela, bien plus qu'il y a quelques années, et les principes d'hygiène informatique commencent à se répandre.

On pourra toujours se poser la question de savoir pourquoi il existe des *hackers*, mais il faut aussi se souvenir de l'attaque de la *CIA*, donc des États-Unis d'Amérique contre les centrifugeuses iraniennes. Cela constitue bien une attaque d'État à État et cela aurait pu aller plus loin. On pointe souvent la Chine d'un doigt accusateur, sans trop de preuves d'ailleurs, et c'est vrai que toute attaque informatique peut retarder un pays tandis que sa sécurité active lui permet de rattraper son retard et, éventuellement, d'aller de l'avant. Cette question ne peut absolument pas être négligée par les gouvernements.

Le rapport peut paraître touffu mais le sujet lui-même est touffu ; il est très compliqué. L'informatique, c'est un peu la loi de la maille et des nœuds en électricité, on ne sait pas où passe l'électricité mais elle arrive au bout. Il en va un peu de même pour l'informatique, sujet très compliqué, car les attaques peuvent venir de partout et même du fabricant qui utilise une porte de derrière prévue pour son seul usage.

On peut avoir des soupçons sur tout, même sur les téléphones ou les tablettes sécurisés de la présidence de la République et du Gouvernement – d'ailleurs plus ou moins utilisés. Finalement, c'est François Mitterrand qui avait raison en estimant que, si quelqu'un a quelque chose d'important à dire à une autre personne, cela doit se faire directement, sans l'écrire, ni téléphoner.

**M. Jean-Yves le Déaut**. – Cela fait penser à cette plaisanterie soviétique : « *Si tu penses quelque chose, ne le dis pas ; si tu le dis, ne l'écris pas ; si tu l'écris, ne le signe pas ; et si tu le signes, ne t'étonne plus de rien* ».

Juste deux petits points de forme encore. Tout d'abord, je trouve que le schéma de la page 48 montrant l'intérieur de la boîte noire du numérique est excellent ; cela représente très bien la complexité du système numérique qui vient d'être évoquée.

Deuxièmement, excusez-moi, c'est un réflexe de professeur qui a assisté à de nombreuses soutenances de thèses, je note que l'acronyme *SCADA*, sa définition, ne figurent pas dans le glossaire. Si j'ai bien compris, il s'agit de données du système de production des entreprises collectées à partir de capteurs que, quelquefois, l'on va chercher sur Internet. Or, si tous les capteurs de machines sensibles sont en lien avec Internet, il peut y avoir, à un moment donné, moyen de capter les données qu'ils transmettent et même d'introduire un espion à l'intérieur du système.

**M. Bruno Sido** : Renseignement pris, *SCADA* signifie « *Supervisory Control and Data Acquisition* », et désigne un logiciel de supervision industrielle tel que vous l'avez parfaitement bien compris. Cette précision figurera dans le glossaire.

**M. Jean-Yves Le Déaut**. – Au terme de cette réunion de travail, nous prenons date pour la présentation d'une version améliorée suivant les indications retenues, en notant qu'il y a déjà eu unanimité pour dire qu'il s'agissait d'un bon travail.

*La séance est levée à 17 heures*

## Membres présents ou excusés

**Office parlementaire d'évaluation des choix scientifiques et technologiques**

Réunion du mercredi 17 décembre 2014 à 16 h 15

Députés

*Présents.* - Mme Anne-Yvonne Le Dain, M. Jean-Yves Le Déaut

*Excusés.* - M. Christian Bataille, M. Alain Marty, Mme Dominique Orliac

Sénateurs

*Présents.* - Mme Marie-Christine Blandin, M. Roland Courteau, M. Bruno Sido

*Excusés.* - Mme Delphine Bataille, Mme Brigitte Gonthier-Maurin, M. Jean-Pierre Leleux, M. Christian Namy