ASSEMBLÉE NATIONALE

XIV^e LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Communication de MM. Bruno Sido, sénateur, et Jean-Yves Le Déaut, député, relative à l'audition publique sur « *le risque numérique, en prendre conscience pour mieux le maîtriser ?* »

Nomination des membres du conseil scientifique .....

Mercredi 26 juin 2013
Séance de 17 heures

Compte rendu n° 35

SESSION ORDINAIRE DE **2012-2013**

Présidence de M. Bruno Sido, sénateur, *Président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mercredi 26 juin 2013

Présidence de M. Bruno Sido, Sénateur, Président

La séance est ouverte à 17 heures

M. Bruno Sido, sénateur, Président. Mes chers collègues, notre ordre du jour comprend deux points : d'abord, une communication relative aux conclusions que Jean-Yves Le Déaut et moi-même pouvons tirer de l'audition publique du 21 février sur « *le risque numérique, en prendre conscience pour mieux le maîtriser ?* ; ensuite, la présentation de nos propositions concernant le renouvellement du Conseil scientifique.

*

– Communication de MM. Bruno Sido, sénateur, et Jean-Yves Le Déaut, député, relative à l'audition publique sur « *le risque numérique, en prendre conscience pour mieux le maîtriser ?* »

M. Bruno Sido, sénateur, président. Je rappelle préalablement que le bureau de l'OPECST a décidé, le 8 septembre 2010, de faire suivre toute audition publique d'actualité, c'est-à-dire toute audition publique non rattachée directement à une étude, d'une présentation devant l'OPECST des conclusions retenues par les rapporteurs, ces conclusions étant publiées en même temps que le contenu des débats.

Le 21 février dernier, l'Office organisait en salle Lamartine, conjointement avec les commissions chargées de la défense de l'Assemblée et du Sénat, une audition publique ouverte à la presse sur le thème suivant : « *Le risque numérique : en prendre conscience pour mieux le maîtriser ?* » Au terme de notre débat, je soumettrai les conclusions de cette audition à votre approbation.

Si le développement exceptionnel des systèmes d'information et de communication, dans toutes les sphères de l'activité humaine, a été très positif en termes de services rendus et d'activité économique générée, il n'en présente pas moins des risques de nature diverses dont le nombre et la gravité s'accroissent plus que proportionnellement à ce développement. Force a été de constater, lors de cette audition, que l'Union européenne et singulièrement la France ont pris du retard dans leurs réponses aux menaces contre les particuliers, les entreprises ou les administrations publiques, civiles ou militaires.

L'actualité renforce chaque jour ce constat. Les chefs d'État du G8, réunis les 17 et 18 juin derniers au Sommet de Lough Erne, en Irlande du Nord, ont signé une charte pour l'ouverture des données publiques. La révélation le 10 juin dernier de la mise en place par l'administration américaine du système « Prism » de surveillance des échanges d'information dans le monde entier renforce le constat établi et l'urgence de la riposte. Aux États-Unis par exemple, le *Patriot Act* permet aux autorités d'accéder aux données stockées par les entreprises sur leur territoire.

L'importance de ce sujet justifie l'annonce d'une prochaine saisine de l'Office par la Commission des affaires économiques du Sénat. Dans cette perspective, la présente communication tente de tirer les premières conclusions issues de la journée d'audition publique du 21 février.

*

* *

L'audition a permis d'abord de faire un état de la réalité des menaces et de présenter les stratégies de réponses.

Les menaces peuvent être de nature militaire ; on parle alors de cyberdéfense, ainsi l'attaque du virus Stuxnet contre le programme nucléaire iranien. Elles peuvent être également de nature civile ; il s'agit alors de cybercriminalité ou de cybersécurité, par exemple l'utilisation frauduleuse des moyens de paiement, le vol de mots de passe, l'écoute des communications téléphoniques, la manipulation de l'information. On a vu récemment l'attaque informatique contre le producteur de pétrole Saudi Aramco, qui l'a handicapé pendant plus d'une semaine. Ou encore l'espionnage de la société AREVA ou de Bercy à la veille de la présidence française du G8/G20. Certaines attaques sont – permettez-moi l'expression – « duales », civiles et militaires : intrusion, espionnage, vol de données, destruction des systèmes d'information, virus… Le CEA serait soumis à des attaques quotidiennes.

La cyberdéfense est considérée par le tout récent Livre blanc sur la défense et la sécurité nationale comme la troisième menace stratégique après l'agression sur le territoire national et l'attaque terroriste et avant la criminalité organisée ou les risques naturels ou industriels. L'État se doit donc de définir une stratégie de réponse et de capacités autonomes de cyberdéfense. Le Président de la République a tout récemment franchi une étape décisive en envisageant la création de capacités non seulement défensives mais aussi offensives en la matière. La création en juillet 2009 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constitué une première réponse ; des moyens renforcés devront lui être affectés, avec par exemple une croissance des effectifs de l'ordre de 50 emplois en temps plein par an au cours des cinq prochaines années. L'ANSSI a une mission de prévention qui passe par la capacité de l'État à édicter des codes de bonne pratique et de promouvoir les audits de cybersécurité. Elle assume aussi une mission de réaction avec des équipes d'intervention aptes à faire face aux attaques toujours plus nombreuses dont sont victimes les entreprises et les administrations. La question de la création d'une cyber-réserve citoyenne devra être posée.

La Commission européenne et le Service européen pour l'action extérieure (SEAE) ont adopté, en février dernier, une stratégie européenne en matière de cyber-sécurité. Ils y préconisent le renforcement des moyens de prévention et d'opposition aux attaques, le développement des ressources industrielles et technologiques en matière de cybersécurité, ainsi que, dans chaque État membre, la création d'une agence de cybersécurité et la définition d'une politique nationale. La stratégie repose sur la coopération entre ces agences nationales avec le soutien de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), crée en 2004. Elle préconise le soutien au développement d'industries « cyber », avec la promotion des investissements dans la R&D.

Cette stratégie européenne vise à créer une « culture du risque » avec un partage d'information entre les secteurs privés et publics. D'importants efforts restent à entreprendre, dans chaque État membre, en matière de sensibilisation de tous les acteurs concernés (grandes

entreprises, PME, administrations publiques, particuliers, utilisateurs…) aux règles élémentaires d'« hygiène » informatique, auxquelles l'ANSSI a récemment consacré un guide. Le constat largement partagé est que la principale source de vulnérabilité réside dans le comportement des personnes, usagers ou employés.

Sur la base de cette stratégie, la Commission européenne a proposé en février dernier une directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union. La disposition phare de cette directive soumettrait les entreprises, les opérateurs d'importance vitale et les administrations à une obligation de signalement des incidents graves aux autorités nationales compétentes. Actuellement seuls les opérateurs de télécommunications sont tenus de le faire. Beaucoup d'entreprises attaquées gardent le silence pour préserver leur crédibilité.

Le renforcement de la sécurité passe maintenant par une action de régulation. La domomédecine (médecine à domicile) présente un bon exemple d'une activité bien régulée, notamment par la loi « informatique et libertés » (sécurité et traçabilité des informations, authentification, droit à l'oubli…). Le dispositif législatif et règlementaire issu du « paquet télécom » européen a donné la capacité de mener des audits auprès des opérateurs de télécommunications, de leur imposer des règles de sécurité et de signaler les incidents majeurs de sécurité. La question se pose maintenant pour les autres opérateurs. En France, la loi, qui protège la vie privée interdit aux opérateurs téléphoniques d'analyser le trafic ; elle empêche ainsi d'avertir de façon proactive leurs clients quand ils sont l'objet d'attaques ou infectés. Or les attaques sont massives et proviennent du monde entier dans les scénarios coordonnés.

Une vigilance particulière doit être portée aux systèmes d'information des secteurs sensibles dans la banque et la finance, l'énergie, les télécommunications, les transports, la santé ou la défense, voire dans certains secteurs de l'industrie. Les menaces sont nombreuses : cyber-espionnage, avec le vol de la propriété intellectuelle et le pillage de secrets industriels, cyber-sabotages ou simples bugs informatiques. Tout dysfonctionnement de ces secteurs d'activité d'importance vitale peut entraîner des conséquences désastreuses pour la nation toute entière.

*
* *

L'audition s'est attachée à analyser la question de la fiabilité et de la sécurité numérique d'une part dans les systèmes militaires, d'autre part, dans les systèmes civils.

Dans le domaine militaire, l'état-major des armées reconnaît que des efforts importants restent à faire pour renforcer la sécurité des systèmes d'information embarqués, notamment concernant les systèmes d'armes et les automatismes des plateformes. Un schéma directeur capacitaire oriente les actions à entreprendre sur un horizon de dix ans. Dans le contexte actuel de forte contrainte budgétaire, doivent être considérés comme prioritaires les investissements planifiés (chiffreurs de données, sondes...), l'effort en R&D sur la cyberdéfense spécifique des systèmes d'armes, ainsi que des experts en sécurité en nombre suffisant et bien formées. Le budget des études amont a doublé en 2013 par rapport à 2012 ; cet effort devra être poursuivi.

L'interconnexion croissante des systèmes numériques militaires nécessite un arbitrage entre gains et risques. La volonté d'embarquer de plus en plus d'intelligence se traduit par des fonctionnalités plus riches, par une certaine complexité et par la nécessité d'interconnexions, de communications et d'ouverture. L'interconnexion des systèmes de

défense est aujourd'hui un fait et une nécessité qui répondent à des impératifs militaires. Pour des raisons budgétaires, mais aussi de performance, les systèmes militaires recourent dans une large mesure à des équipements civils ou dérivés du monde civil. La question de l'interopérabilité avec nos alliés est très importante. L'emploi de technologies civiles dans les systèmes d'armement a accru considérablement leurs performances mais est aussi une source majeure de vulnérabilité. Pour bénéficier de l'apport de ces technologies tout en assurant la sécurité il faut établir une chaîne de confiance, un écosystème industriel qui s'inscrit dans la durée. Cela suppose le développement de champions nationaux avec, là aussi, la nécessité de mise en œuvre d'une véritable politique industrielle. Il nous faut garder en France et en Europe la maîtrise des technologies critiques et des capacités de production des systèmes d'information utilisés dans l'armement. L'ANSSI et le ministère de la Défense ont chacun un rôle à jouer dans l'établissement d'un partenariat de confiance.

S'agissant de la sûreté numérique des systèmes civils, un facteur important de vulnérabilité réside dans les terminaux BOYD (*bring your own device*) ; en effet nous utilisons de plus en plus nos téléphones, tablettes ou ordinateurs personnels pour travailler. Le risque est d'autant plus grand que les systèmes de ces terminaux sont contrôlés par un très petit nombre d'acteurs, essentiellement Google et Apple.

La panne du 6 juillet 2012, qui a entraîné l'indisponibilité du réseau Orange pendant 11 heures, n'était pas le résultat d'une attaque mais d'une panne technique. Si les systèmes informatiques du secteur aéronautique sont fiables, grâce à des méthodes de développement et de certification sophistiquées, qu'en est-il de ceux des secteurs médical, automobile ou des téléphones portables ? Dans ces trois domaines, où les normes sont insuffisantes, la nécessité économique de réduire les coûts entraîne la multiplication des bugs informatiques.

La sûreté numérique représente des enjeux majeurs pour notre économie et nos emplois dans ce qu'il n'est pas trop fort d'appeler une « guerre économique ». Certains évoquent la possibilité d'interdire à l'échelle nationale ou européenne le déploiement ou l'utilisation de routeurs et autres équipements de cœur de réseau d'origine chinoise.

L'accumulation actuelle de couches logicielles de fournisseurs différents, et de plus en plus complexes, rend plus difficile la tâche de sortir un produit sans vulnérabilité logicielle. La même vulnérabilité concerne la chaîne des sous-traitants. Tous les interstices sont des sources potentielles de vulnérabilité. Ainsi de nombreuses failles sont-elles récemment apparues dans le langage Java très largement utilisé. La confiance dans la chaîne d'approvisionnement est essentielle ; asseoir cette confiance mérite donc la mise en œuvre d'une politique industrielle à l'échelle nationale. Il est en outre essentiel de pouvoir certifier ces différents éléments ; les normes de sécurité sont des éléments structurants de la mise en place des processus de certification.

L'excellence de la recherche française en mathématiques a permis de développer des instruments comme l'analyse statique et la vérification par méthode formelle, qui s'assurent de la validité des systèmes d'information. Il s'agit de produire des systèmes qui s'approchent du « zéro défaut ». Faut-il conclure positivement de cet avantage en disant qu'il y a, dans notre pays, un véritable potentiel de développement pour une industrie dans ce domaine ? Ou alors constater, une fois de plus, notre faiblesse à valoriser l'innovation et la recherche ? La dizaine de sociétés françaises qui commercialisent ces technologies restent de taille modeste, entre 10 et 200 personnes.

Plusieurs intervenants de l'audition publique ont fait le constat que notre capacité de formation n'est pas à la hauteur en termes quantitatifs. D'après une estimation menée par l'ANSSI et les industriels, la formation d'experts en sécurité ne correspond qu'à un quart des besoins. Les cours de cybersécurité devraient devenir obligatoires dans les écoles d'ingénieurs et d'informaticiens. Nous devons créer de nouvelles filières universitaires qui nous permettrons d'accroître le nombre de spécialistes en ces domaines. L'effort de R&D est également insuffisant ; il doit être soutenu pour maîtriser certaines technologies fondamentales : cryptologie, architecture matérielle et logicielle, équipements de sécurité et de détection… ; la recherche doit être duale en favorisant les synergies entre industries civiles et militaires.

*
* *

L'audition du 21 février a enfin permis une première analyse du rôle de l'utilisateur individuel dans la sécurité des systèmes numériques, sous les divers angles du risque d'addiction, du développement des réseaux sociaux et de la protection des données personnelles.

Le développement des réseaux sociaux, des systèmes de télésurveillance ou de géolocalisation a entraîné une dissémination sans précédent des données personnelles. L'absence de protection juridique par des sociétés basées hors de France présente des risques majeurs pour le respect de la vie privée. Beaucoup de sites internet revendiquent la propriété pure et simple des données à caractère personnel postées par les internautes. Présentée par la Commission européenne en janvier 2012, la proposition de règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit : une plus grande transparence dans l'utilisation des données ; le consentement explicite au traitement des données personnelles ; l'accès à ces données ; et un droit à l'oubli numérique. La proposition prévoit que les règles de l'Union devront s'appliquer si des données à caractère personnel font l'objet d'un traitement à l'étranger par des entreprises implantées sur le marché européen et proposant leurs services aux citoyens de l'Union. Il est dès lors regrettable que son adoption ait été tout récemment rejetée en raison de désaccords entre États membres.

Les phénomènes d'addiction à l'Internet et singulièrement aux réseaux sociaux se développent. Il ressort de l'audition publique qu'il faut parler de dépendance plutôt que d'une réelle addiction aux conséquences néfastes (consommation croissante, sentiment de privation, consommation compulsive aux conséquences néfastes sur les plans personnel, sanitaire, professionnel financier et juridique). Il n'en reste pas moins vrai que d'énormes progrès doivent être faits dans les familles et au sein de l'Éducation nationale pour enseigner aux jeunes gens les dangers, les risques et la bonne utilisation de l'Internet. Les « comportement numériques » doivent toutefois être étudiés et enseignés dans les cursus des spécialistes du comportement humain, en liaison avec les spécialistes de la sécurité informatique.

L'information vaut beaucoup d'argent, elle est devenue le nouveau pétrole. Les services de la société de l'information comme les moteurs de recherche, les réseaux sociaux, les messageries, le stockage dans le nuage (*cloud*) ou les systèmes de vente en ligne ont connu un développement prodigieux en l'espace de quelques années. Le potentiel d'extraction automatique de connaissances à partir de ces données est considérable. Or les informations ainsi stockées ou échangées sont gérées principalement par des sociétés américaines (Google, Amazon, Facebook, Apple – « GAFA »), qui s'en réservent la propriété et l'exploitation, souvent à l'insu des utilisateurs. Ce *leadership* américain dans la capacité de récolter et de

traiter la donnée mondiale (*big data*) soulève un problème de souveraineté dans tous les pays d'Europe. La Chine, le Japon, la Corée, la Russie ont mieux résisté, avec des produits alternatifs locaux. On ne peut que saluer la création de sociétés françaises comme CloudWatt qui dote notre pays de solution de « nuage » (*cloud*) sécurisées.

Se pose également la question de la gouvernance de l'Internet. En dépit de quelques évolutions, le dispositif actuel, fondé sur des initiatives d'industriels américains privés, reste insuffisant. Ainsi en l'absence de système officiel d'authentification de l'identité numérique, le Royaume-Uni envisage d'utiliser le service d'authentification de Facebook pour l'accès aux services publics en ligne.

*
* *

En conclusion, on constate que la société de l'information se développe très rapidement hors de l'Europe. Deux questions essentielles pourraient dès lors servir de fil directeur à la prochaine étude de l'OPECST : l'Europe ne risque-t-elle pas d'entrer dans une forme de sous-développement à cet égard ? Est-il encore temps de réagir pour favoriser l'émergence d'entreprises européennes dans ces secteurs ?

M. Jean-Pierre-Leleux, sénateur.- Le monde de la culture a été en émoi depuis un an et demi à propos de l'exception culturelle. Peut-on considérer qu'il y a, au travers de l'économie numérique, un risque de nature culturelle, par exemple pour diffuser notre message patrimonial et historique ?

M. Bruno Sido.- C'est une excellente question. Elle n'a pas été évoquée lors de l'audition publique, mais devra l'être dans les travaux futurs de l'Office sur ce sujet.

M. Gérard Bapt, député.- Je m'étais intéressé à la cybersécurité pour les données du dossier médical personnalisé (DMP) qui sont échangées sur messagerie. La valeur des données de santé se mesure en milliards de dollars. Leur sécurité et leur hébergement constituent donc un enjeu important. Au-delà des actes de sabotage, la cybersécurité des données de santé est souvent un problème de formation ou d'erreur humaine. Au tout récent salon aéronautique du Bourget, les réseaux des opérateurs SFR et Orange étaient saturés, mais je dois reconnaître que ce n'était ni un bug ni un sabotage.

M. Bruno Sido.- Les intervenants de l'audition publique ont effectivement estimé que les secteurs de la santé, de l'automobile et de la téléphonie mobile étaient parmi les plus vulnérables en termes de sécurité informatique. Les bénéfices des systèmes d'information nous exposent aux risques de manipulation et de malveillance.

M. Gérard Bapt.- Je rajouterais aussi le risque d'incompétence. Un exemple récent a vu le DMP d'un patient publié sur l'Internet. Après enquête, il s'est avéré que cela avait été le fait involontaire d'un sous-traitant privé du CHU travaillant sur le suivi clinique d'une cohorte de femmes enceintes.

Mme Catherine Procaccia, sénatrice.- Les erreurs ou malveillances existaient avant la création de l'Internet, il suffisait d'envoyer un courrier confidentiel avec une mauvaise adresse sur l'enveloppe. La différence est qu'avec l'Internet on peut toucher beaucoup plus de personnes. Je ne suis pas sûre que ce soient les jeunes, nés avec l'Internet, qui ont le plus besoin de formation. Les personnes « dépendantes » de l'Internet se situent davantage dans la tranche d'âge 24 – 45 ans et ils sont tout aussi imprudents. En outre, ce sont

eux qui sont en possession des données professionnelles les plus sensibles. Il faudrait réfléchir à l'idée de rendre les formations obligatoires dans les entreprises.

D'autre part, n'est-il pas déjà trop tard pour que des entreprises françaises ou européennes concurrencent les leaders américains de l'Internet ? Nous ne pouvons faire comme d'autres pays qui se permettent de contrôler la circulation de l'information sur les réseaux. L'administration française pourrait-elle obliger ses agents à utiliser des outils sécurisés ou plus protecteurs des données personnelles ? Je constate dans l'administration et les cabinets ministériels une utilisation généralisée des téléphones – assistants personnel (*Smartphones*) connectés à l'Internet, alors que cela était interdit il y a encore quelques années.

Qui trop embrasse mal étreint : pourrait-on envisager d'imposer un niveau de sécurité à certains secteurs ciblés, comme la santé, à l'instar de ce qui se fait pour le secteur aéronautique ?

M. Bruno Sido.- Les employés d'AREVA et du Commissariat à l'énergie atomique (CEA) ont reçu l'instruction de couper la fonction Wifi de leurs téléphones – assistants personnels et de leurs ordinateurs portables. En effet les données échangées sur les liaisons Wifi circulent de façon non sécurisée. Les jeunes sont plus enclins à exposer leur vie privée sur les réseaux sociaux ; un effort de formation leur sera donc utile tout au long de leur vie. Mais vous avez raison, il faut former toutes les tranches d'âge.

Je distingue les opérateurs français et étrangers. Peut-on être sûrs des opérateurs qui ne sont pas français, qu'ils soient européens ou pas ?

M. Gérard Bapt, député.- Les hébergeurs de données françaises doivent être agréés par le ministère de la Santé ou par la Commission nationale de l'informatique et des libertés (CNIL).

M. Bruno Sido.- Il faudra effectivement développer les normes et les systèmes de certification. Nous venons de découvrir que la NSA (*National Security Agency*) américaine surveillait tout le monde sans *corpus* législatif approprié. C'est un domaine très vulnérable et la première des protections consiste à être tous mobilisés sur le sujet.

Mme Delphine Bataille, sénatrice.- Le sous-développement européen est réel par rapport à la suprématie américaine. La stratégie européenne est de renforcer les moyens de prévention : création d'une agence de cybersécurité dans chaque État membre, efforts importants de sensibilisation en direction de tous les acteurs, qu'ils soient publics ou privés. Dans l'état actuel des choses, y a-t-il d'autres État membres qui seraient plus avancés que la France, comme par exemple l'Allemagne ?

M. Bruno Sido, sénateur, président.- Cette question n'a pas été évoquée lors de l'audition publique et elle mérite une recherche. Hors Europe, nous savons que la Chine est très avancée en ces domaines ; nous nous méfions de ses routeurs car comment savoir les destinations vers lesquelles les informations sont finalement routées… Et que fait réellement la NSA américaine ? On voit bien que les risques encourus sont maintenant partout et potentiellement très importants. Tous ces sujets méritent une étude plus approfondie de l'Office.

Les conclusions de l'audition publique sont adoptées à l'unanimité des membres présents.

*

– Nomination des membres du conseil scientifique

M. Bruno Sido, sénateur, président. - Nous en arrivons maintenant au renouvellement du Conseil scientifique. Je rappelle que ce Conseil a été institué en même temps que l'OPECST en 1983, pour lui porter toute l'assistance scientifique nécessaire, à sa discrétion.

En pratique, il est réuni au moins deux fois l'an pour faire un point sur les sujets d'actualité scientifique pouvant utilement faire l'objet de futurs travaux de l'OPECST, sous forme d'études (sous réserve bien entendu de la transmission d'une saisine) ou sous forme d'auditions publiques d'actualité ; pour ce dernier cas, je citerai l'exemple de deux auditions publiques organisées en octobre 2010 sur les apports des sciences et technologies à l'évolution des marchés financiers, ou en mars 2011 sur les terres rares.

Nous ne manquons pas d'associer aussi notre Conseil scientifique à des moments importants d'échanges comme lors de la formulation de notre avis sur la stratégie nationale de recherche et d'innovation en 2009, ou lors de la visite à l'Assemblée nationale des lauréats français de la médaille Fields en novembre 2010.

Par ailleurs, le Conseil scientifique est un relais permanent vers la Communauté scientifique et technologique pour la recherche de contacts utiles pour nos rapporteurs.

La loi fixe à trois ans la durée du mandat d'un Conseil scientifique. Il est composé de vingt-quatre personnalités choisies en raison de leurs compétences dans les domaines des sciences et de la technologie. Le règlement intérieur de l'OPECST prévoit qu'il est nommé par la délégation, sur proposition du président et du premier vice-président.

Le dernier renouvellement datant de 2010, Jean-Yves Le Déaut et moi avons donc procédé à des consultations permettant de faire une place à des personnalités émergentes, qui seront appelées à devenir à leur tour des ambassadeurs de l'OPECST dans les milieux scientifiques et professionnels qui sont les leurs.

La nouvelle composition proposée comporte douze nouvelles personnalités, ce qui correspond à un renouvellement de moitié. Le nombre de femmes est doublé, puisqu'elles constitueront un tiers de l'effectif total, contre un sixième auparavant.

COMPOSITION CONSEIL SCIENTIFIQUE 2013

Nom des conseillers	année de nomination	spécialités
Mme Hélène BERGÈS	2013	INRA Toulouse - ADN
Mme Catherine BRÉCHIGNAC	2010	Secrétaire perpétuelle de l'Académie des sciences, ancienne présidente du CNRS – Physique atomique
M. Gérald BRONNER	2013	Professeur de sociologie, Université Paris-Diderot

Mme Bernadette CHARLEUX	2013	Directrice du Laboratoire de Chimie, Catalyse, Polymères & Procédés - Lyon 1 - CNRS
M. Hervé CHNEIWEISS	2003	Directeur de recherche au CNRS, directeur du laboratoire « Plasticité gliale » à l'INSERM-Université Paris Descartes – Neurobiologie, Neurologie
M. Michel COSNARD	2013	PDG Inria – Sciences de l'informatique
M. Jean-Marc EGLY	2003	Membre de l'Académie des sciences, directeur de recherche à l'INSERM – Chimie, Biochimie
M. Jean-Pierre FINANCE	2003	Représentant permanent de la Conférence des présidents d'université (CPU) auprès de l'UE à Bruxelles – Informatique, Mathématiques
M. Jean-Pierre GATTUSO	2013	Directeur de recherche au CNRS - Océanographie
M. Laurent GOUZENES	2003	Conseiller du président de Pacte Novation et expert scientifique du groupe - Robotique et Intelligence artificielle
Mme Claudie HAIGNERÉ	2007	Ancien ministre, membre de l'Académie des technologies, présidente d'Universcience - Rhumatologie, Neurosciences, Astronautique
Mme Edith HEARD	2013	Professeure au Collège de France directrice de l'unité « Génétique et biologie du développement » à l'Institut Curie, CNRS-INSERM
M. Étienne KLEIN	2003	Directeur du laboratoire de recherche sur les sciences de la matière du CEA, professeur de physique et de philosophie des sciences à l'École centrale de Paris
M. Daniel KOFMAN	2003	Professeur à Telecom parisTech, co-fondateur et directeur du LINCS (Laboratory of Information, Networking and Communication Sciences)
Mme Marie-Christine LEMARDELEY	2013	Présidente de l'Université Sorbonne Nouvelle - Paris 3 - Littérature américaine contemporaine
M. Stéphane MANGIN	2013	Professeur de physique, Université de Lorraine, Institut Jean Lamour-CNRS, Institut Universitaire de France
Mme Valérie MASSON-DELMOTTE	2013	Directrice du Laboratoire des sciences du climat et l'environnement-CEA
Mme Dominique MEYER	2010	Membre de l'Académie des sciences, professeure à la faculté de médecine à l'Université Paris-Sud Orsay
M. Jean-François MINSTER	2003	Membre de l'Académie des sciences, membre de l'Académie des technologies, directeur scientifique du groupe Total
M. Olivier OUILLÉ	2013	Professeur à l'Université d'Aix-Marseille, Fédération de recherche CNRS « Comportement, Cerveau & Cognition » et

		Laboratoire de psychologie cognitive
M. Bruno REVELLIN-FALCOZ	2010	Président honoraire de l'Académie des technologies - Aéronautique
M. Gérard ROUCAIROL	2010	Président de l'Académie des technologies - Sciences de l'informatique
M. Marcel VAN DE VOORDE	2013	Professeur à l'Université technologique de Delft, Pays-Bas - Nanotechnologies
M. Cédric VILLANI	2013	Médaille Field 2010 Directeur de l'Institut Henri Poincaré

M. Bruno Sido, sénateur, président. - Certaines nouvelles figures sont en fait déjà des fidèles compagnons de route de l'OPECST, qui se sont déjà illustrés par leur motivation au service de nos rapporteurs lors d'auditions publiques ou de visites sur place. À partir des biographies jointes, vous constaterez que tous ont une solide assise dans leur discipline, et que la plupart des domaines des sciences de la nature, des sciences du vivant et des sciences de l'homme sont couverts.

Tous les membres du Conseil scientifique reconduits sont volontaires, et ont manifesté à la fois de l'assiduité et de la réactivité au cours du mandat écoulé.

Vous observerez en outre que la liste des personnalités proposées assure des liens avec les principales institutions de la recherche et de l'enseignement supérieur en France, voire avec les sphères de la gouvernance communautaire de la recherche, dans le cas de M. Marcel Van de Voorde. Nous avons veillé à intégrer à la fois des professeurs d'université, et des dirigeants de la recherche en industrie.

J'ouvre maintenant la discussion sachant que nous sommes ensuite appelés à nous prononcer sur cette liste par un vote global, puisque l'établissement en incombe au Président et au Premier vice-président.

Mme Catherine Procaccia, sénatrice. – Cette liste ne semble comporter qu'un seul responsable de recherche industrielle. N'est-ce pas faire une place insuffisante à la recherche en entreprise ?

M. Bruno Sido, sénateur, président. – En fait, les deux membres président et président honoraire de l'Académie des technologies sont d'anciens dirigeants de l'industrie.

M. Gérard Bapt, député.- Je me réjouis de voir figurer dans cette liste l'INRA de Toulouse, qui joue un rôle crucial dans l'étude des canaux de diffusion du bisphénol A dans le corps humain : paroi intestinale, peau, (manipulation des tickets de caisse) et, selon une étude récente, muqueuse de la bouche.

Mme Catherine Procaccia, sénatrice. – Tout en convenant qu'il incombe de faire des choix, je regrette que cette composition n'intègre pas un chercheur du CIRAD (Centre de coopération internationale en recherche agronomique pour le développement). Mais ce pourrait être une suggestion pour le prochain renouvellement dans trois ans. Par ailleurs, je m'interroge sur la « plasticité gliale », spécialité de M. Hervé Chneiweiss.

M. Bruno Sido, sénateur, président. – M. Hervé Chneiweiss, outre ses compétences de premier ordre en neurobiologie, qui en fait un participant régulier aux auditions publiques de l'OPECST, est depuis peu président du comité d'éthique de l'INSERM.

La nouvelle composition du Conseil scientifique est adoptée à l'unanimité des membres présents.

M. Bruno Sido, sénateur, président. – J'indique que le nouveau Conseil scientifique sera réuni le 9 juillet, à 18 heures, pour une discussion sur les thèmes d'actualité scientifique pouvant utilement mobiliser l'OPECST. Cet échange sera suivi, vers 19 h 30, d'un cocktail auquel nous avons invité les membres sortant du Conseil scientifique pour bien marquer que les liens de confiance créés restent durables.

La séance est levée à 18 heures

Membres présents ou excusés

Office parlementaire d'évaluation des choix scientifiques et technologiques

Réunion du mercredi 26 juin 2013 à 17 heures

Députés

Présent. - M. Gérard Bapt

Excusés. - M. Alain Claeys, Mme Anne Grommerch, M. Jean-Yves Le Déaut, M. Alain Marty

Sénateurs

Présents. - Mme Delphine Bataille, M. Roland Courteau, M. Jean-Pierre Leleux, Mme Catherine Procaccia, M. Bruno Sido

Excusés. - Mme Corinne Bouchoux, M. Marcel Deneux, Mme Virginie Klès, M. Jean-Claude Lenoir