N° 1221

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958
QUATORZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale
le 3 juillet 2013

N° 721

SÉNAT

SESSION EXTRAORDINAIRE 2012-2013

Enregistré à la présidence du Sénat
le 3 juillet 2013

**OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES**

RAPPORT

sur

LE RISQUE NUMÉRIQUE : EN PRENDRE CONSCIENCE POUR MIEUX LE MAÎTRISER ?

Compte rendu de l'audition publique du 21 février 2013 et de la présentation des conclusions le 26 juin 2013

Par MM. Bruno SIDO, sénateur, et Jean-Yves LE DÉAUT, député

Déposé sur le Bureau de l'Assemblée nationale
par M. Jean-Yves LE DÉAUT,

Premier Vice-président de l'Office

Déposé sur le Bureau du Sénat
par M. Bruno SIDO,

Président de l'Office

Composition de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

Président

M. Bruno SIDO, sénateur

Premier Vice-président

M. Jean-Yves LE DÉAUT, député

Vice-présidents

M. Christian BATAILLE, député
Mme Anne-Yvonne LE DAIN, députée
M. Jean-Sébastien VIALATTE, député
M. Roland COURTEAU, sénateur
M. Marcel DENEUX, sénateur
Mme Virginie KLÈS, sénatrice

DÉPUTÉS	SÉNATEURS
M. Gérard BAPT	M. Gilbert BARBIER
M. Christian BATAILLE	Mme Delphine BATAILLE
M. Denis BAUPIN	M. Michel BERSON
M. Alain CLAEYS	Mme Corinne BOUCHOUX
M. Claude de GANAY	M. Marcel-Pierre CLÉACH
Mme Anne GROMMERCH	M. Roland COURTEAU
Mme Françoise GUEGOT	Mme Michèle DEMISSINE
M. Patrick HETZEL	M. Marcel DENEUX
M. Laurent KALINOWSKI	Mme Chantal JOUANNO
Mme Anne-Yvonne LE DAIN	Mme Fabienne KELLER
M. Jean-Yves LE DEAUT	Mme Virginie KLES
M. Alain MARTY	M. Jean-Pierre LELEUX
M. Philippe NAUCHE	M. Jean-Claude LENOIR
Mme Maud OLIVIER	Mme Marie-Noëlle LIENEMANN
Mme Dominique ORLIAC	M. Christian NAMY
M. Bertrand PANCHER	M. Jean-Marc PASTOR
M. Jean-Louis TOURAINE	Mme Catherine PROCACCIA
M. Jean-Sébastien VIALATTE	M. Bruno SIDO

SOMMAIRE

—

Pages

PREMIÈRE PARTIE :
LA PLACE DU NUMÉRIQUE DANS LA GESTION DE LA MENACE STRATÉGIQUE

I. PREMIÈRE TABLE RONDE : ÉTAT DES LIEUX EN MATIÈRE DE CYBERSÉCURITÉ

Présidence de M. Jean-Louis Carrère, président de la Commission des affaires étrangères, de la défense et des forces armées du Sénat

Introduction par M. Bruno Sido, sénateur, président de l'OPECST

M. Bruno Sido, sénateur, président de l'OPECST. Je me réjouis que le Parlement puisse tenir une telle audition publique, à l'initiative de l'Office parlementaire d'évaluation des choix scientifiques et technologiques.

Regrouper notre délégation et les commissions de la défense et des forces armées de l'Assemblée nationale et des affaires étrangères, de la défense et des forces armées du Sénat est, au demeurant, une métaphore des travaux que nous menons en commun à l'Office, entre députés et sénateurs.

Actuellement, nous sommes ainsi chargés de quatre études, qui sont chacune portées par deux rapporteurs – un sénateur et un député.

Mais le sujet que nous allons aborder est tellement central pour notre pays que nous aurions aussi bien pu y associer des membres des commissions des affaires économiques, tant la pénétration diffuse de la numérisation est devenue décisive pour notre compétitivité, ou des affaires culturelles, puisqu'on ne peut aujourd'hui pratiquement plus faire de recherche de haut niveau sans avoir recours à des modélisations de plus en plus sophistiquées.

Mais Chamfort se rappelle à moi, qui disait « *pour le superflu, il faut s'en tenir au nécessaire* ». C'est pourquoi je termine ici mon propos introductif. Je m'exprimerai sur le fond du sujet lors de la première table ronde de cet après-midi.

M. Jean-Louis Carrère, président de la commission des affaires étrangères, de la défense et des forces armées du Sénat, président. Permettez-moi tout d'abord de féliciter notre collègue Bruno Sido pour son

initiative, mais aussi de remercier l'Assemblée nationale, en particulier Mme Patricia Adam et M. Jean-Yves Le Déaut pour la qualité de leur accueil.

La menace représentée par les attaques contre les systèmes d'information n’est pas un sujet nouveau pour la commission des affaires étrangères et de la défense du Sénat. Dès 2007, après les attaques massives subies par l'Estonie, elle avait commencé à s'intéresser à ce sujet et avait publié un premier rapport d'information sur la cyberdéfense, présenté par notre ancien collègue Roger Romani.

Beaucoup de choses se sont passées depuis cinq ans. On peut notamment citer le cas de Stuxnet, ce virus informatique qui aurait contribué à retarder l'avancement du programme nucléaire militaire de l'Iran, en s'attaquant à des centrifugeuses d'enrichissement de l'uranium.

C'est la raison pour laquelle nous avons jugé utile de réactualiser ce rapport, notamment dans l'optique de l'élaboration du nouveau Livre blanc sur la défense et la sécurité nationale. Notre collègue Jean-Marie Bockel s'est donc vu confier la mission de rédiger un nouveau rapport sur la cyberdéfense, qu'il a présenté devant notre commission en juillet dernier et dont les conclusions ont été adoptées à l'unanimité.

Pour avoir été membre – avec Mme Patricia Adam et plusieurs de nos collègues députés et sénateurs – de la commission chargée d'élaborer le nouveau Livre blanc, et même si sa version définitive n'a pas encore été publiée, je pense pouvoir dire ici que la cyberdéfense devrait être l'une de ses priorités, et qu’il devrait se traduire par une nouvelle impulsion dans ce domaine.

Ces dernières années, les attaques contre les systèmes d'information se sont en effet multipliées, qu'il s'agisse de cybercriminalité, de tentatives de déstabilisation, d'affaires d'espionnage, ou de sabotage à des fins de destruction. Je pense notamment à l'attaque informatique qui a visé l'été dernier l'un des premiers producteurs de pétrole, Saudi Aramco.

Notre pays n'est pas à l'abri de ce fléau, comme en témoignent les affaires d'espionnage de Bercy – survenues à la veille de la présidence française du G8 et du G20 – ou d'AREVA.

C'est l'objet de cette première table ronde que d'essayer de cerner l'étendue effective de la menace que représentent les atteintes à la sécurité des systèmes numériques stratégiques.

Nous allons tenter d'évaluer la portée de cette menace grâce à nos trois premiers intervenants. M. Pascal Chauve, du Secrétariat général de la défense et de la sécurité nationale, va s'efforcer d’en rendre compte sous l'angle global de son intensité et de son acuité. M. Stéphane Grumbach, directeur de recherche à

l'INRIA, analysera dans quelle mesure l'importance de cette menace peut s'interpréter comme le résultat d'une véritable géopolitique des données numériques gérée à l'échelle des grands pays. Enfin, M. Frédéric Hannoyer, de ST Microelectronics, évoquera les multiples canaux techniques qu'elle peut emprunter pour prendre forme.

Afin de laisser place au débat, j'invite les différents intervenants à limiter leur temps de parole à dix minutes.

M. Pascal Chauve, Secrétariat général de la défense et de la sécurité nationale (SGDSN). Ma tâche est à la fois facile et difficile. Parler de la menace est certes toujours plus facile que d'évoquer les réponses qui peuvent lui être apportées, mais je dois aussi, dans un contexte particulièrement inquiétant, me garder de faire trop peur et veiller à donner la juste mesure de cette menace. Mon point de vue est celui du SGDSN : il s'attache à des problématiques et à des enjeux de sécurité nationale.

Lorsqu'on évoque la menace informatique, on pense d'emblée à ce qui nous affecte dans notre vie quotidienne, par exemple les virus qui viennent « écraser » les photos des enfants sur le disque dur de l'ordinateur, ou encore la cybercriminalité qui touche les individus – vol de données bancaires, utilisation frauduleuse des moyens de paiement, accès à nos comptes en ligne – et qui appelle des réponses de nature policière.

Mais la menace informatique ne vise pas que les individus, et n'a pas pour seul objectif l'appât du gain. Elle peut revêtir une tout autre dimension, qui dépasse la cybercriminalité, et viser des activités critiques pour le fonctionnement d'une nation, qui relèvent pleinement d'une problématique de sécurité nationale. Des exemples viennent d'en être donnés.

S'il fallait dresser une typologie des menaces auxquelles une Nation peut être exposée, je distinguerais trois domaines. Le premier est celui de la simple revendication, dans lequel les attaquants vont afficher des messages sur des sites officiels ou gouvernementaux en réponse à une politique à laquelle ils sont opposés – c'est ce que l'on appelle la défiguration de site. Ils utilisent les vulnérabilités habituelles des serveurs web pour s'y introduire. Récemment, lors de l'opération Serval au Mali, des groupes d'activistes se sont ainsi attaqués à des sites web plus ou moins officiels, sans toutefois causer de dommages particuliers, pour afficher leurs revendications.

La deuxième forme de menace informatique qui peut revêtir des enjeux nationaux est bien sûr le cyber-espionnage. Je ne parle pas du vol d'informations personnelles à des individus, mais du cyber-espionnage à grande échelle, qui peut toucher des entreprises, notamment celles qui travaillent dans les secteurs sensibles, ou des opérateurs relevant de ce que nous appelons les secteurs d'activité d'importance vitale, parmi lesquels figurent la banque, l'énergie, les

transports ou la défense. Il y a là des acteurs économiques et des opérateurs qui détiennent des secrets de fabrication ou des secrets de fonctionnement d'une autre société. L'espionnage dont a été victime la société AREVA figure dans le rapport sur la cyberdéfense du sénateur Bockel, ainsi que celui qui a touché Bercy. Si vous avez lu la presse des derniers jours, vous avez appris que la société américaine Mandiant aurait trouvé l'origine d'une campagne d'espionnage informatique systématique conduite chez des industriels américains – 141 cas ont été rapportés. Ce pillage de secrets industriels aurait une origine étatique – je vous laisse découvrir laquelle.

S'agissant de cyber espionnage, la presse ne révèle cependant que la partie émergée de l'iceberg. Le SGDSN, avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), traite de très nombreux cas qui sont couverts par le secret, les opérateurs ne souhaitant pas que l'on fasse état des atteintes qu'ils subissent. Je vous confirme que cette menace n'est pas potentielle, mais quasi systématique.

La nouvelle forme de menace informatique qui touche les intérêts souverains est le cyber-sabotage. La transition entre le cyber-espionnage et le cyber-sabotage est désormais consommée. Vous vous souvenez sans doute du ver Slammer, qui avait semé « la pagaille » dans le système informatique de distribution d'électricité de l'Ohio et entraîné un blackout touchant 50 millions d'abonnés américains en 2003. Telle n'était peut-être pas l'intention de départ, mais toujours est-il qu'il est possible de toucher, par des moyens informatiques, des secteurs d'activité d'importance vitale dans leur fonctionnement, mettant ainsi en péril des fonctions vitales de la nation.

Comment a-t-on pu passer d'une menace potentielle, qui n'occupait que les esprits des spécialistes, à une menace réelle ? La technologie et les usages nous exposent de plus en plus à ces menaces. D'une part nous faisons face à un empilement de technologies de plus en plus chancelant ; il faut rétablir la chaîne de la confiance entre des systèmes d'exploitation du matériel, des applications, des middleware, qui vivent chacun sur une couche d'abstraction de la couche qui est en dessous, interprètent les commandes, et laissent finalement autant d'interstices à l'attaquant pour s'infiltrer dans les systèmes. D'autre part, c'est le problème de la confiance dans la chaîne d'approvisionnement de nos systèmes informatiques et de la maîtrise technologique qui est posé. Je vous rappellerai à cet égard le bon mot fait par Ken Thompson, gourou de la sécurité informatique, en 1984 : « *Vous ne pouvez pas faire confiance à un code dont vous n'êtes pas totalement l'auteur, surtout si vous faites appel à des sociétés qui emploient des gens comme moi* ». La confiance dans la chaîne d'approvisionnement est vitale. Asseoir cette confiance mérite donc la mise en œuvre d'une politique industrielle à l'échelle nationale.

L'usage moderne des technologies de l'information est désormais de tout interconnecter avec tout, et donc d'offrir autant de voies d'attaque à des agents

menaçants. Il est aussi caractérisé par la mobilité, qui fait circuler les technologies, les informations et les virus d'un système à l'autre, et par l'introduction de systèmes informatiques à vocation personnelle dans des applications professionnelles. Je pense au *bring your own device* (BYOD), qui fait que certains d'entre nous travaillent avec leurs terminaux personnels, qui sont autant de vecteurs d'infection, infection à l'échelle de l'individu mais qui peut ensuite se propager à l'échelle nationale.

M. Stéphane Grumbach, INRIA, directeur de recherche. J'évoquerai pour ma part les données et leur répartition sur la planète.

La société de l'information offre des services comme les moteurs de recherche, les réseaux sociaux ou les systèmes de vente en ligne, qui sont devenus incontournables – peu différents, en définitive, de nos utilities – comme disent les Anglais – telles que l'eau ou l'électricité. Pour leurs utilisateurs, ces services sont essentiellement gratuits. Les sociétés qui les proposent assurent le stockage et le traitement des données, avec en général une très grande qualité de service. D'un point de vue économique, on ne peut cependant pas exactement considérer ces services comme gratuits. Les utilisateurs échangent avec les entreprises leurs données privées contre des services. Ces données, qui peuvent sembler bien anodines, s'avèrent parfois d'une grande valeur. C'est par exemple le cas des requêtes sur un moteur de recherche, utilisées pour établir des profils utilisateurs qui permettent de cibler efficacement la publicité. Elles peuvent aussi l'être pour extraire des connaissances bien plus riches que les profils personnels – j'y reviendrai cet après-midi.

Certains systèmes stockent des données dont le caractère personnel est plus immédiat. C'est le cas des réseaux sociaux, au premier rang desquels Facebook, grâce auxquels les utilisateurs mettent à disposition toutes sortes d'informations personnelles. Les réseaux sociaux conservent également la structuration des relations sociales entre leurs utilisateurs, leurs échanges et, au-delà, leurs interactions avec d'autres services. Mais Facebook est bien plus qu'un réseau social : c'est le système numérique du futur, celui dans lequel nous stockerons nos données, et au moyen duquel nous interagirons avec le monde. C'est le système qu'utiliseront de nombreuses entreprises pour développer des services qui exploiteront l'interface et les fonctionnalités de Facebook. Facebook peut disparaître, mais ce type de système perdurera pour devenir universel.

Deux évolutions majeures dans la technologie induisent des changements fondamentaux dans la gestion des données. Tout d'abord, la disparition annoncée de nos ordinateurs conduira, tant pour les individus que pour les organisations, à une gestion des données et des services dans le nuage, données et services qui seront accessibles de n'importe où, au moyen de n'importe quelle tablette. Ensuite, le développement massif des réseaux sans fil qui forment l'infrastructure des

services mobiles introduit une rupture dans la société de l'information, en assurant des services au plus près des individus.

Les données personnelles sont devenues la ressource essentielle de cette nouvelle industrie. Assez similaire aux matières premières pour l'industrie traditionnelle, cette ressource sera un jour plus importante pour l'économie globale que le pétrole. Être capable de la récolter et de la transformer pour en faire des produits est donc d'une importance capitale. Au-delà de la ressource, ces données sont aussi une monnaie avec laquelle les utilisateurs payent leurs services. Cette monnaie, potentiellement dé-corrélée des banques centrales, sera conduite à jouer un rôle croissant.

La concentration est une caractéristique importante des industries de la société de l'information. Facebook a dépassé le milliard d'utilisateurs ; Google agrège de nombreuses activités – moteur de recherche, messagerie, réseau social, mobilité. Dans la société de l'information, la taille des entreprises est déterminante. La quantité de données et le nombre d'utilisateurs qu'elles gèrent contribuent exponentiellement à leur puissance.

Dans ce nouvel écosystème, les données circulent et passent les frontières. Certaines régions les accumulent, les traitent et les contrôlent, d'autres non. Comme pour les échanges commerciaux, on peut distinguer les exportations et les importations. Mais contrairement au commerce, les mouvements de données se font surtout gratuitement, c'est-à-dire sans paiement de l'exportateur par l'importateur. Les données ne font à ce jour pas l'objet d'un marché au niveau mondial : il n'y a pas de bourse de la donnée comme il en existe pour les matières premières.

Les États-Unis ont un véritable leadership dans la capacité à récolter et à traiter la donnée mondiale. Ils ont toujours fait preuve d'un véritable génie dans le développement des services de la société de l'information. Ils inventent des services extraordinaires, comme le démontre la rapidité de leur adoption, assurent une qualité de service inégalée – tout le monde utilise Gmail – et savent construire des modèles économiques efficaces.

Une cartographie des flux de données au niveau planétaire, sur le modèle des cartographies des flux de matières premières, serait extrêmement utile. Elle n'est aujourd’hui pas facile à établir. On peut toutefois étudier les services qui sont utilisés dans les différentes régions, qui constituent un premier indicateur assez significatif. Aux États-Unis, les 25 premiers sites de la toile sont tous américains. En France, comme dans un certain nombre de pays européens, seulement le tiers des 25 premiers sites sont français ; les autres sont américains. En outre, les premiers sites français ne sont pas les plus gros accumulateurs de données.

La situation est plus contrastée en Asie. En Chine, l'industrie nationale domine la toile, avec des systèmes très puissants et diversifiés dans tous les secteurs. Au Japon et en Corée, de nombreux systèmes, aussi fondamentaux que les réseaux sociaux, sont des systèmes locaux.

Si l'on considère les moteurs de recherche, qui jouent un rôle si essentiel dans notre accès à l'information, la situation de l'Europe, région de la diversité culturelle, est surprenante. Google y détient plus de 90 % de parts de marché. Ce n'est pourtant pas le cas aux États-Unis, où Bing et Yahoo ont chacun près de 15 % de parts de marché. La Chine et la Russie ont quant à elles développé deux des plus grands moteurs mondiaux : Baidu, qui détient 78 % du marché chinois, et Yandex, qui détient 60 % du marché russe.

Ces chiffres sont corroborés par l'analyse globale des premiers systèmes mondiaux, c'est-à-dire ceux ayant le plus grand nombre d'utilisateurs dans le monde. Parmi les cinquante premiers, on trouve 72 % d'Américains, 16 % de Chinois, 6 % de Russes, mais seulement 4 % d'Européens.

Les études que nous avons faites sur la partie invisible de la toile, celle des trackers qui permettent de suivre l'activité des utilisateurs au moyen de systèmes tiers, confirment cette tendance. Là encore, les Américains dominent largement ces systèmes invisibles, subtils accumulateurs de données.

Certaines régions envisagent la révolution numérique avec enthousiasme, d'autres avec crainte. Le programme de cette journée, centré sur la menace stratégique et le risque de dépendance, révèle le positionnement plutôt sur la défensive de la France. La situation de l'Europe est paradoxale : si le taux de pénétration est fort et les infrastructures importantes, aucun des grands systèmes de la toile n'est développé sur notre continent. Les données personnelles, pétrole de la nouvelle économie, sont la pierre d'achoppement des Européens, qui restent focalisés sur les dangers de leurs utilisations potentielles, en particulier pour la vie privée. La société de l'information se développe donc hors de l'Europe. On peut dire sans exagération que celle-ci est entrée dans une forme de sous-développement en dépendant, pour des services dont l'importance ne fait que croître, d'une industrie étrangère.

L'Europe exporte donc ses données aux États-Unis. Mais il y a autre chose : elle n'en importe pas. Or la capacité à récolter des données à l'étranger est également stratégique : elle permet de créer de la valeur à partir de ressources qui arrivent gratuitement, et de dégager des connaissances dans tous les domaines sur les régions dont viennent les données.

Les Américains ont une stratégie très élaborée en la matière, comme le montre leur succès international. Permettez-moi de l'illustrer par un exemple encore peu visible. À l'heure où la possibilité d'ouverture de la Corée du Nord fait frémir les chancelleries et où les Chinois construisent des infrastructures à la

frontière, Google cartographie le territoire. Les cartes Google deviendront probablement incontournables lors du développement du pays. Et comme leur intérêt est avant tout l'hébergement des applications des entreprises, Google héritera d'une capacité d'analyse de la Corée, grâce aux flux de données qui transitent par ses machines. Le marché en Corée du Nord est de surcroît loin d'être facile pour les Américains, tant les Coréens du Sud et les Chinois sont de puissants concurrents.

Les exemples asiatiques pourraient être intéressants pour les Européens. Ces pays ont bien compris les enjeux de la société de l'information ; ils préservent une certaine souveraineté en offrant tous les services de l'Internet made in Asia. En même temps ; ils ont une forte connexion avec la recherche américaine. En Chine, les laboratoires d'Alibaba ou de Baidu sont peuplés de chercheurs de la Silicon Valley – les mêmes que chez Facebook ou Google : ils participent du même écosystème.

J'aborderai cet après-midi les nouveaux services de la société de l'information, qui reposent sur ces données et dont nous dépendrons à l'avenir.

M. Frédéric Hannoyer, ST Microelectronics, directeur de recherche. Je vous remercie de m'offrir l'occasion de témoigner au nom de ST Microelectronics.

Vous m'assignez une tâche difficile. Je vais me livrer à une présentation rapide, qui ne pourra être exhaustive, en m'efforçant de ne pas être trop technique. J'essaierai de couvrir les grandes familles d'attaques à partir d'exemples récents. Dans la mesure où les attaques stratégiques ont été traitées par M. Chauve, je me concentrerai davantage sur des exemples d'attaques contre les particuliers et les entreprises.

Une attaque peut être définie comme une intrusion sur un système de sécurité qui génère un dommage ou un préjudice. Une intrusion élémentaire peut être décomposée en trois composantes : au moins une vulnérabilité dans le logiciel ou le système ; un vecteur – qui est souvent un programme – qui utilise et exploite cette vulnérabilité, qui arrive à passer à travers les mesures de sécurité mises en œuvre, et qui installe un composant actif, un programme malware, qui est la partie maligne de l'attaque. Soit ce programme lance une autre attaque de l'intérieur du système, soit il effectue sa mission – récolte des mots de passe, analyse du réseau ou du système, écoute des communications – et reporte à l'attaquant. Le composant actif peut soit être autonome, soit être commandé de l'extérieur. Il peut remplir ses missions tout de suite, ou rester silencieux pendant très longtemps – jusqu'à des années. Le rapport de Mandiant[1] cite ainsi des attaques où les

[1] *"Unit 61398: A Chinese cyber espionage unit on the outskirts of Shanghai?" – http://nakedsecurity.sophos.com/2013/02/19/unit-61398-chinese-military-cyber-espionage-unit/*

composants actifs sont restés inactifs pendant plusieurs années, mais étaient fréquemment questionnés.

Parmi les préjudices subis figure le vol d'argent aux particuliers ou aux entreprises, par exemple avec des malwares tels que Zeus ou Citadel grâce à la récupération des mots de passe temporaires envoyés par les banques, type 3D secure, le vol de propriété artistique, auquel nous avons été sensibilisés par la loi HADOPI, l'espionnage de données ou vol de propriété intellectuelle – secrets d'affaires ou de production. Un exemple en a récemment été fourni par une intrusion sur le site du New York Times1 visant à connaître la teneur des articles en préparation sur le Premier ministre chinois. Les communications téléphoniques sont exposées maintenant aux mêmes attaques que les données pures.

De nouvelles attaques apparaissent : le chantage aux données personnelles des particuliers[2], assorti d'une demande de rançon ; le sabotage de services, qui empêche l'activité économique, et offre la possibilité de détruire une infrastructure de production, ce qui peut avoir un coût considérable pour une entreprise ; les attaques à la réputation. Nous voyons également se développer la désinformation par le piratage des médias sociaux, comme Twitter. Nous en avons constaté l'impact en ce qui concerne la population en Inde[3] , mais aussi les marchés économiques, comme le marché du pétrole – le piratage du compte Twitter d'un diplomate Russe[4] annonçant la mort du Président syrien Bashar Al-Assad a par exemple créé des remous sur les marchés du pétrole.

Parmi les futures attaques à redouter, on peut penser à la santé. La démonstration que l'on peut envoyer une décharge par le piratage de pacemakers à une dizaine de mètres doit nous faire réfléchir, de même que le fait que tous les équipements médicaux soient connectés à Internet pour pouvoir récupérer des mises à jour de logiciels. Je pense également à la domotique. Comment réagirait une caserne de pompiers si toutes les alarmes incendie d'une ville se déclenchaient en même temps ?

Les attaques peuvent être distinguées selon le point d'attaque. Celui-ci peut être situé dans le terminal, qu'il s'agisse d'un ordinateur, d'un compteur électrique, d'un téléphone, ou de tout navigateur web. Il peut être situé dans le centre de données lui-même, où les mots de passe ou les informations dans le

---

[1] *"Hackers in China attacked the Times for last four months"*

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

[2] *http://www.arstechnica.com/tech-policy/2013/01/california-man-finally-arrested-after-sextorting-over-350-women/*

[3] *India Asks Pakistan to Investigate Root of Panic," by Jim Yardley, The New York Times, August 19, 2012:*

http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html

[4] *"Twitter Rumor Sparked Oil-Price Spike," by Nicole Friedman, WSJ.com, August 6, 2012:*

http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html

nuage sont stockées, ou enfin dans le réseau – d'où on peut facilement rediriger les communications d'une victime vers le PC d'un attaquant ou écouter les messages en clair.

La sécurité se doit de couvrir les trois maillons de cette chaîne, le terminal, le centre de données, et le réseau. Les vulnérabilités utilisées peuvent être scindées en deux catégories : celles qui peuvent être traitées par une mise à jour des logiciels, et celles pour lesquelles cette mise à jour s'avère délicate ou ne suffit pas.

Pour ce qui est des premières, l'accumulation actuelle de couches logicielles de fournisseurs différents, et de plus en plus complexes, rend la tâche de sortir un produit sans vulnérabilité logicielle impossible. Une vulnérabilité du logiciel est juste un bug non fonctionnel, qui ne crée donc pas de problème dans l'utilisation de l'application, mais est exploité par le pirate pour prendre le contrôle et compromettre l'équipement – car il a alors tous les pouvoirs. On a parlé dernièrement de la vulnérabilité de la technologie Java dans le navigateur web, et des attaques de Facebook et d'Apple[1].

Ces vulnérabilités logicielles sont très nombreuses. Elles peuvent être traitées. Mais avant cela, elles créent des exploits « zero day », qui peuvent se définir comme l'exploitation d'une faille qui n'est pas publique, indétectable donc par les équipements de sécurité, et qui concerne même les plateformes bénéficiant des dernières mises à jour. Les exploits « zero day » sont devenus un phénomène courant, qui bénéficie même d'une chaîne de valeur et d'un marché pour les développer et les revendre[2]. Ils doivent être traités sérieusement. C'est pourquoi il est essentiel de pouvoir mettre à jour les plateformes de manière très réactive et à distance.

Parmi les autres vulnérabilités à traiter, je citerai les vulnérabilités sur la chaîne de production chez les sous-traitants, et les équipements qui pourraient être piégés[3]. C'est pourquoi il faut garder une maîtrise industrielle dans les produits. Lorsque l'ensemble de notre cœur de réseau sera chinois ou américain, quelle confiance pourrons-nous réellement lui accorder ? Il nous faut au moins arriver à construire cette confiance.

Je pense aussi aux attaques de cryptographie et aux attaques sur les certificats[4], qui sont les bases de la confiance sur les échanges numériques, ou

---

[1] *"Apple computers'hacked' in breach" - http://www.bbc.co.uk/news/technology-21510791*

[2] *"Welcome to the Malware-Industrial Complex" | MIT Technology Review – http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/*

[3] *"Huawei and ZTE pose security threat, warns US panel"*

[4] *"Security firm Bit9 hacked, Stolen Digital Certs Used To Sign Malware" – Hacking News http://thehackernews.com/2013/02/security-firm-bit9-hacked-stolen.html*

encore aux attaques sur la vulnérabilité humaine – mots de passe devinables, complicités internes…

Le critère majeur est à mon sens la grande furtivité des attaques. Les malware peuvent s'attraper en surfant nos sites préférés[1] ou en ouvrant un attachement ou un lien dynamique dans un email, ils peuvent se mettre en dessous du système d'opération et des systèmes de sécurité. Ils s'interfacent entre vous et le matériel, par exemple lorsque vous tapez votre code confidentiel sur votre téléphone ou sur un terminal de paiement, ou lorsque votre logiciel vous donne des informations confidentielles, ou lorsque vous communiquez au niveau du réseau. Ils sont aussi capables de dissimuler toutes leurs actions des mécanismes de surveillance du terminal.

M. le président Jean-Louis Carrère. Je vous remercie de vos interventions. Après avoir identifié les menaces, nous allons tenter d'identifier les stratégies de réponse. Pour cela, je donnerai successivement la parole à M. Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est l'autorité nationale chargée de la protection et de la défense des systèmes d'information, à M. Jean-Marie Bockel, sénateur, à M. Eduardo Rihan Cypel, député, et enfin au capitaine de vaisseau Alexis Latty, de l'état-major des armées.

M. Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il n'est pas aisé d'expliquer comment il convient de réagir face au tableau cataclysmique qui vient de nous être présenté. Si quelqu'un, où qu'il se trouve, pense avoir la bonne réponse, je l'invite à contacter l'ANSSI au plus vite : nous avons un poste à lui proposer ! (*Sourires*.)

La stratégie de réponse de l'État a cependant évolué de manière significative depuis quelques années. La problématique de la sécurité de nos données n'est certes pas nouvelle, puisque des systèmes de chiffrement sont apparus dès l'Antiquité, mais le sujet a littéralement explosé depuis quelques années. La stratégie nationale de la France a véritablement commencé à évoluer à partir de 2008 et du dernier Livre blanc sur la défense et la sécurité nationale, qui a identifié le risque d'attaque majeure contre les systèmes d'information comme une menace stratégique, et estimé que le degré de probabilité d'occurrence dans les quinze années à venir était extrêmement fort. Il était dès lors nécessaire de se doter d'une stratégie et de capacités de cyberdéfense.

---

[1] *2013 Cisco Annual Security Report – « Online shopping sites are 21 times more likely to deliver malicious content than counterfeit software sites.»:"As Cisco data shows, the notion that malware infections most commonly result from "risky" sites such as counterfeit software is a misconception. Cisco's analysis indicates that the vast majority of web malware encounters actually occur via legitimate browsing of mainstream websites. In other words, the majority of encounters happen in the places that online users visit the most—and think are safe".*

La stratégie, définie dans la foulée du Livre blanc sur la défense et la sécurité nationale de 2008, repose sur quatre points. En premier lieu, la France souhaite être une puissance mondiale en matière de cyberdéfense. Il ne s'agit pas de montrer notre force pour le plaisir. Simplement, les frontières n'existent pas dans ce domaine. On ne peut donc se contenter d'être un joueur local.

En deuxième lieu, il s'agit de conserver la capacité – que la France avait par le passé – de protéger ses informations essentielles de manière autonome. On touche ici au cœur du cœur du fonctionnement de l'État dans les domaines de la défense et de la sécurité nationale. Pour prendre un exemple, nous devons être capables de produire des chiffreurs en toute autonomie, afin d'être sûrs de ne pas dépendre de tiers auxquels nous ne faisons pas nécessairement confiance.

En troisième lieu, nous devons renforcer très significativement la sécurité de nos infrastructures vitales. J'aime à dire que les systèmes d'information et de télécoms sont nos systèmes nerveux : rien ne fonctionne dans notre vie courante sans informatique. Si nous ne sommes pas capables de protéger les infrastructures vitales que sont la distribution d'énergie, les moyens de télécommunication, nos finances, nos systèmes médicaux et nos systèmes industriels, notre Nation s'effondrera.

Enfin, il nous faut promouvoir la sécurité dans le cyberespace. Nous sommes là dans l'usage du citoyen, et de la confiance qu'il peut avoir dans l'e-administration et les transactions sur Internet.

Pour mettre en œuvre cette stratégie, nous avons établi – comme toujours en France, mais à raison me semble-t-il – une capacité centralisée. Nos grands homologues internationaux ont souvent davantage d'effectifs que nous, mais ils sont généralement moins centralisés.

Créée en 2009, l'ANSSI est à la fois l'autorité de sécurité et l'autorité de défense. Elle a donc deux missions, une mission de prévention et une mission de réaction.

La mission de prévention consiste à veiller à ce que nos infrastructures vitales, qu'elles soient gouvernementales ou privées, soient suffisamment résilientes et capables de résister à des attaques informatiques. Cela repose sur un ensemble d'actions, dont la principale est le conseil, c'est-à-dire la capacité de l'État à édicter de bonnes pratiques en matière de règles de sécurité et à délivrer des labels à des produits de sécurité ou à des prestataires. Un grand nombre de prestataires coexistent en effet dans le domaine de la cybersécurité, un peu moins dans celui de la cyberdéfense ; il faut pouvoir s'y retrouver. La capacité à aller vérifier participe aussi de la prévention – c'est ce que l'on appelle l'audit. Concrètement, il s'agit de tests de pénétration consistant à vérifier si nos systèmes étatiques ou les systèmes critiques privés sont capables de résister à des attaques informatiques. Je ne détaillerai pas les résultats – qui ne sont pas vraiment

brillants. Il y a enfin notre capacité à doter le cœur de l'État de moyens de haute sécurité, pour qu'en cas de problème, nos autorités puissent continuer à communiquer et à échanger de l'information en toute sécurité.

Malheureusement, cette mission de prévention, qui représenterait 90 % de notre activité dans un monde stable, est largement supplantée par l'autre activité de l'ANSSI : l'activité de réaction, à savoir la responsabilité, sous l'autorité du Premier ministre et du secrétaire général de la défense et de la sécurité nationale, de coordonner et de piloter la réponse lorsque les infrastructures critiques ou les grandes entreprises françaises sont touchées. Cette activité repose sur un centre opérationnel localisé aux Invalides, actif vingt-quatre heures sur vingt-quatre. Notre capacité de réaction et de défense est hélas « enfoncée » par le volume des attaques informatiques, si bien que nous devons en permanence arbitrer entre les différentes attaques pour décider de celles sur lesquelles nous devons nous mobiliser. Notre action est ici facile à comprendre. Elle 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. Cela nécessite d'abord de comprendre ce qui se passe, en sachant que le pirate peut être présent dans l'entreprise depuis très longtemps – jusqu'à quatre ans, selon le rapport de Mandiant. Il faut ensuite comprendre ce qu'il fait et où il a déposé les virus informatiques. Une fois ceux-ci identifiés, il faut nettoyer le réseau. Dans le cas des très grandes entreprises, ce sont plusieurs centaines de milliers d'ordinateurs qui peuvent être potentiellement infectés. La dernière mission consiste à remettre en état et à re-sécuriser le réseau. Si vous réinstallez le réseau tel qu'il était après une attaque informatique, ce que vous avez fait ne servira en effet pas à grand-chose : les attaquants – qui travaillent souvent en toute impunité – recommenceront immédiatement à exploiter vos vulnérabilités.

M. Jean-Marie Bockel, sénateur. Je n'insisterai pas sur le constat – cela a été fait, et fort bien, par les intervenants précédents – mais sur les avancées que je tiens à saluer et sur les progrès qui restent à accomplir.

Nous sommes dans un contexte particulier. Cette rencontre est la bienvenue à la veille de la publication du Livre blanc sur la défense et la sécurité nationale. Dans le rapport d'information sur la cyberdéfense que j'ai présenté au nom de la commission des affaires étrangères et de la défense du Sénat, j'ai abordé le sujet du risque numérique sous l'angle de la défense, mais c'est un sujet transversal, qui touche à nos intérêts vitaux, mais aussi à l'économie, à la vie quotidienne de nos concitoyens et aux services publics. Le Livre blanc sera donc une étape importante, et ce que nous disons dans cette dernière ligne droite revêt par conséquent un sens particulier.

S'agissant de notre stratégie de réponse, nous observons un certain nombre d'avancées. J'avais appelé, à l'image de ce que font les Britanniques ou les

Allemands, à ériger la cyberdéfense en une priorité nationale portée au plus haut niveau de l'État. Nous avons progressé sur ce point : le président de la République François Hollande a explicitement évoqué cet enjeu dans la lettre de mission adressée à M. Jean-Marie Guéhenno – président de la commission chargée de rédiger le Livre blanc – comme dans ses vœux aux armées.

La question des moyens de l'ANSSI est évidemment centrale. Les États qui réduisent aujourd'hui leurs dépenses de défense, notamment en Europe, n'en augmentent pas moins les budgets dédiés aux outils en matière de cyberdéfense et de cybersécurité. Sans parler des États-Unis, on peut citer le cas du Royaume-Uni. Dans un tel contexte, les moyens de l'ANSSI ont vocation à se renforcer pour être portés au niveau de ceux de nos partenaires britannique ou allemand. La qualité de notre outil est reconnue, y compris à l'international, mais ses moyens sont encore insuffisants. Je me félicite donc de la création de 65 postes supplémentaires à l'ANSSI en 2013 ; ses effectifs devraient atteindre 500 agents à l'horizon 2015. Nous serons bientôt au même niveau que nos voisins non plus sur le seul plan qualitatif, mais aussi sur le plan quantitatif. Le ministre de la défense, M. Jean-Yves Le Drian, a également annoncé un renforcement des effectifs des armées dans le domaine de la cyberdéfense.

Mon rapport proposait aussi de créer une « cyber réserve » citoyenne, qui rassemble des spécialistes et des ingénieurs mobilisés sur ces questions. Cette proposition peut sembler anecdotique de prime abord, mais je crois savoir que l'état-major la prend très au sérieux.

J'en viens aux évolutions législatives ou réglementaires qui permettraient à ces outils publics de mieux exercer leurs missions. Lors de la réunion du Forum international de la cybersécurité (FIC) à Lille, le ministre de l'intérieur, M. Manuel Valls, a annoncé la création d'un groupe interministériel chargé d'étudier l'adaptation de notre droit aux nouvelles menaces liées au cyber. D'autres progrès pourront être envisagés dans le cadre de la future loi de programmation militaire.

Je m'étais montré assez critique en ce qui concerne le niveau européen, mais je me félicite aujourd'hui de la publication, le 7 février, de la nouvelle stratégie de l'Union européenne en matière de cybersécurité, qui s'accompagne d'une proposition de directive. Le président M. Jean-Louis Carrère m'a d'ailleurs désigné pour suivre ce sujet pour la commission des affaires étrangères, de la défense et des forces armées du Sénat avec notre collègue Jacques Berthou. Compte tenu des compétences de l'Union en matière de normes, de réglementation et de communication, il était important qu'elle se positionne sur ce sujet. Il y a d'ailleurs un lien entre législation nationale et européenne sur un point que j'avais mis en exergue, l'obligation de déclaration d'incident, notamment pour les entreprises et les opérateurs d'importance vitale. Lorsque ceux-ci sont attaqués, ils ont tendance à taire ce qu'ils considèrent comme un signe de faiblesse, qui

pourrait leur faire perdre des marchés. Or c'est le contraire : plus ils ont de valeur, plus ils seront attaqués. Ils doivent donc l'assumer et accepter de se faire aider. L'obligation de déclaration d'incident les y aidera.

Après ces motifs de satisfaction, j'en viens aux aspects de mon rapport qui mériteraient d'être mieux pris en compte.

Tout d'abord, d'importants efforts restent à faire en matière de sensibilisation des administrations, du monde de l'entreprise, notamment des PME, et des opérateurs d'importance vitale. Je pense à l'organisation à l'intérieur des entreprises ou à la place donnée aux responsables des systèmes de sécurité. Ce n'est pas un enjeu technique, mais bien un enjeu économique ; nous sommes en guerre économique, et c'est notre chaîne de valeur qui est concernée. Les exemples qui ont été cités montrent que nous sommes confrontés à un véritable pillage. C'est donc un enjeu majeur pour notre économie et pour la préservation de nos emplois.

Il y a un lien entre cet aspect défensif et les opportunités de développement industriel et de création d'emplois qualifiés. Puisque nous avons parlé de l'actualité, permettez-moi d'évoquer l'entreprise chinoise ZTE, qui hésite toujours à s'implanter à Poitiers. Hier, notre collègue l'ancien Premier ministre Jean-Pierre Raffarin a estimé dans un quotidien local que mon rapport tenait des propos de café du Commerce sur ces sujets. L'actualité d'aujourd'hui – je pense au rapport de Mandiant, qui affirme sans ambiguïté l'existence d'un immeuble abritant des escouades entières de hackers à Shanghai – me donne raison. Je suis un ami de la Chine et je souhaite que l'on commerce avec elle ; ZTE est une belle entreprise. Pour autant, il ne faut pas être naïf : nous devons mettre en place un certain nombre de règles du jeu.

Un point a fait polémique dans mon rapport : la proposition d'interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation des routeurs et autres équipements de cœur de réseau d'origine chinoise qui présentent un risque pour la sécurité nationale dans le contexte actuel. L'aspect positif dans tout cela, c'est que nous devons conforter notre outil industriel, tant au niveau français qu'au niveau européen. Nous avons de beaux fleurons – Thales, Cassidian, Bull, Sogeti ou Alcatel-Lucent – et de nombreuses PME innovantes. Sachons exploiter ces atouts.

Il y a là un enjeu de souveraineté nationale, voire de souveraineté européenne partagée. Nous avons déjà une Europe de l'aéronautique et une Europe spatiale. Pourquoi pas une Europe des industries de la cyber demain ? Le potentiel de développement et de création d'emplois est considérable. Il reste que notre capacité de formation n'est pas à la hauteur en termes quantitatifs, comme en témoigne la difficulté de l'ANSSI à recruter. Or les perspectives sont réelles dans des domaines comme la cryptologie, l'architecture matérielle et logicielle et la production de certains équipements de sécurité ou de détection. Nous sommes

performants, et les échanges avec les Chinois, les Américains ou les Russes existent pour certains produits. Mais sur les routeurs et les équipements de cœur de réseau, nous devons construire pour demain, à partir de nos fleurons, une capacité française et européenne.

Nous avons aujourd'hui une base industrielle et technologique de défense (BITD). Pourquoi ne pas avoir demain une base industrielle et technologique en matière de cyber (BITC) ? Le séminaire gouvernemental du 28 février et la feuille de route pour le numérique devraient nous permettre d'avancer sur ce sujet. Vous recevrez d'ailleurs tout à l'heure la ministre chargée de l'économie numérique, Mme Fleur Pellerin, qui est sensibilisée à cette question ; des progrès importants sont possibles.

Il me paraît également nécessaire de renforcer la sensibilisation des utilisateurs au respect des règles élémentaires de sécurité, que Patrick Pailloux appelle à juste titre des règles d'hygiène élémentaires.

Il nous faut enfin poser la question – sensible – de nos capacités offensives. La France dispose de capacités offensives. Si nous n'avons pas à mettre sur la place publique le dispositif opérationnel qui est le nôtre, qui est un vrai dispositif de dissuasion, nous pourrions néanmoins avoir une doctrine d'emploi. Devant la grande vulnérabilité de nos sociétés, et la possibilité d'une déstabilisation qui confinerait quasiment à une cyber-guerre, les efforts de sensibilisation que nous poursuivons à travers une réunion comme celle-ci ont toute leur importance.

M. le président Jean-Louis Carrère. Je vais maintenant passer la parole à M. Eduardo Rihan Cypel, député de la Seine-et-Marne et membre de la commission chargée d'élaborer le Livre blanc sur la défense et la sécurité. Lors de la réunion de cette commission le 24 septembre dernier, M. Rihan Cypel a rappelé l'urgence d'une réaction nationale face aux menaces d'attaques stratégiques dans le domaine numérique.

M. Eduardo Rihan Cypel, député. Peut-être serai-je amené à répéter certains aspects des interventions précédentes : c'est le signe que nous sommes d'accord sur les problématiques et les enjeux fondamentaux en matière de cybersécurité.

Depuis que je travaille à ces sujets, c'est-à-dire depuis mon élection en juin dernier, j'ai pu mesurer leur importance dans l'organisation de l'ensemble de la société. L'accélération de la révolution amorcée il y a une trentaine d'années a provoqué des bouleversements sociaux considérables. Tout est intégré aujourd'hui, ce qui pose avec force la question de la sécurité des réseaux et de l'acheminement de l'information, mais aussi celle de la sécurité de l'information elle-même.

De la protection du simple citoyen à la sécurité nationale et internationale, les enjeux sont multiples. Les spécialistes en ont une conscience claire : pour eux, ces enjeux ne sont pas seulement virtuels, ils sont aussi d'ordre physique et matériel. Les attaques contre nos systèmes d'information peuvent mettre à bas les circuits numériques pour nous empêcher de communiquer, pour récolter des informations dans le cadre de l'intelligence économique, pour déstabiliser les réseaux ; mais il est également possible, par exemple, d'ouvrir les vannes d'un barrage après avoir pris le contrôle de son système informatique, ou de s'emparer d'un système de contrôle de transports ferroviaires pour provoquer des accidents.

On se souvient du virus Stuxnet, qui a provoqué la désynchronisation des centrifugeuses iraniennes destinées à l'enrichissement de l'uranium et la destruction de 20 à 30 % de ces équipements. La dernière attaque de grande ampleur est celle qui a été menée l'été dernier contre la compagnie pétrolière saoudienne Aramco, infectant 30 000 ordinateurs de l'entreprise. On le voit, les cyberattaques peuvent quasiment provoquer un choc pétrolier.

Le cyberterrorisme prendra très probablement de l'importance dans les années à venir. Nous devons nous préparer à y faire face en mobilisant tous les efforts de la nation. Le Livre blanc de 2008 avait identifié ces sujets comme majeurs, les plaçant presque au même niveau que la dissuasion nucléaire et les forces balistiques conventionnelles. Cela représentait une prise de conscience importante.

Aujourd'hui, nous devons tenir trois enjeux principaux.

D'abord la sécurité nationale. Si l'ANSSI est au cœur de ce combat pour ce qui est de la protection de l'appareil d'État et des grandes entreprises, il reste du travail à accomplir dans tous les segments de la société française : je pense par exemple aux PME exposées au risque d'espionnage économique mais aussi aux particuliers confrontés à la cybercriminalité – près 10 millions de Français ont été victimes de cyberescroqueries l'année dernière pour un coût total estimé à 2,5 milliards d'euros –, notamment par défaut de sécurisation de leurs données bancaires et personnelles. Même si des progrès existent, la prise de conscience est encore insuffisante pour permettre une mobilisation nationale. Je souscris à l'idée selon laquelle la sécurité numérique est un enjeu d'indépendance nationale. La France doit prendre cette question à bras-le-corps.

Les travaux préparatoires au prochain Livre blanc accordent une importance centrale à la cybersécurité. Si je suis confiant de ce point de vue, je pense aussi que la formation est insuffisante.

Le deuxième enjeu est donc celui de la formation. Nous devons créer des filières universitaires qui nous permettront d'accroître le nombre d'ingénieurs dans ce domaine.

Le troisième enjeu est économique. Les questions de sécurité représentent une opportunité formidable pour créer de nouvelles filières économiques et industrielles. Les entreprises qui évoluent dans le secteur présentent des taux de croissance à deux chiffres. Nous avons des atouts – Cassidian, Thales et beaucoup d'autres –, mais il faut encore nous mobiliser car le travail ne fait que commencer.

M. le président Jean-Louis Carrère. Cette mobilisation ne devra pas se relâcher après la remise du Livre blanc : il faut que la loi de programmation qui s'ensuivra corresponde à la volonté politique exprimée dans ce document.

Le capitaine de vaisseau Alexis Latty, de l'état-major des armées, va maintenant nous présenter le dispositif de cyberdéfense des armées, qui est dirigé par le contre-amiral Arnaud Coustillière, officier général à la cyberdéfense.

M. le capitaine de vaisseau Alexis Latty, état-major des armées. Comme l'ont montré les précédents intervenants, le cyberespace est devenu un nouveau lieu de confrontation.

Cette situation est appréhendée par le ministère de la défense selon une approche prioritairement opérationnelle.

Pour la sphère militaire, les enjeux relèvent de l'efficacité de notre outil de défense. Nous devons d'abord protéger les données classifiées ; ensuite être en mesure de continuer à opérer sous agression cybernétique afin de garantir notre autonomie d'appréciation de la situation et notre liberté d'action ; enfin, nous devons contribuer à assurer le bon fonctionnement de l'État en cas de crise cybernétique nationale majeure.

Les théâtres d'opérations cybernétiques – c'est là l'une de leur principale spécificité – englobent non seulement le théâtre classique d'une opération extérieure mais aussi le territoire national. L'exemple malien en est l'illustration la plus récente, avec des cyberattaques – d'ailleurs peu sophistiquées et d'ampleur limitée – contre des intérêts français en réaction à l'opération Serval.

Il faut reconnaître que l'état de cybersécurité du ministère de la défense, en dépit des efforts consentis depuis dix ans, n'est pas encore à la hauteur des risques et des menaces. Nous savons qu'un effort particulier doit être consenti sur les systèmes d'information embarqués, notamment concernant les systèmes d'armes et les automatismes des plateformes.

L'ambition du ministère, en totale adéquation avec les objectifs de la stratégie nationale, est de porter rapidement la cybersécurité au niveau adéquat puis de devenir un acteur majeur de la dimension « cyber » d'une coalition militaire internationale.

Pour y parvenir, nous avons retenu une approche globale. Un schéma directeur capacitaire oriente les actions à entreprendre sur un horizon de dix ans. Il

appréhende l'ensemble des systèmes d'information du ministère, dans l'acception la plus extensive possible en raison non seulement du caractère centralisé de la chaîne opérationnelle de cyberdéfense, mais aussi de l'interdépendance des processus de cyberdéfense et de cyberprotection qui a été précédemment évoquée par le directeur de l'ANSSI.

Concernant les moyens, je soulignerai trois points.

Premièrement, notre organisation a été refondue en 2011. La chaîne opérationnelle de cyberdéfense est désormais centralisée sous l'autorité du chef d'état-major des armées. La chaîne fonctionnelle de cyberprotection est distribuée autour de cinq autorités qualifiées qui ont pour mission de mettre en état de cybersécurité les systèmes d'information dont elles sont responsables.

Deuxièmement, des investissements sont planifiés selon des modalités qui devront être confirmées par la loi de programmation militaire. Ils ménagent un équilibre entre, d'une part, l'acquisition des outils urgents ou indispensables, comme des chiffreurs de données, des sondes sur les systèmes et des logiciels d'analyse technique, et, d'autre part, des dépenses d'avenir visant à étudier la cyberdéfense spécifique des systèmes d'armes et à préparer les outils de demain.

Troisièmement, le renforcement de nos liens avec l'ANSSI s'illustre de manière exemplaire par la co-localisation en 2013 du centre d'analyse et de lutte informatique défensive du ministère avec le centre opérationnel de l'Agence, dans le cadre d'un partenariat de confiance inscrit dans la durée.

Cette politique ambitieuse passe par le développement de relations étroites avec des partenaires internationaux de confiance. Les exigences de souveraineté étant fortes – ce domaine fait partie du premier cercle de souveraineté, au même titre que la dissuasion –, l'orientation principale est de rechercher des convergences avec les partenaires qui ont le même niveau d'ambition, sans toutefois s'en rendre dépendant.

Dans les quelques minutes qui me restent, je voudrais rapidement développer un angle particulier, celui de l'adéquation des ressources humaines aux ambitions

Nous le savons, la cybersécurité repose pour une large part sur des hommes et des femmes. Aujourd'hui nous disposons d'environ 1 000 spécialistes à temps partiel, soit l'équivalent d'environ 300 postes à temps plein. Pour la période 2013-2020, un plan de renforcement de l'ordre de 400 spécialistes pour les armées a été engagé. Ce plan, qui devra également être confirmé par la loi de programmation militaire, vise à professionnaliser la fonction de cybersécurité au rythme d'environ 50 spécialistes additionnels à temps complet par an, qui est le rythme maximum de ce qu'il est possible de consentir.

Les facteurs de succès en manière de ressources humaines reposent sur plusieurs éléments.

En premier lieu, une gestion prévisionnelle performante des effectifs, des emplois et des compétences. Le modèle de ressources humaines des armées reposant sur la génération de compétences en interne, le plan de renforcement CYBER est une opportunité pour remodeler les parcours professionnels et la pyramide des emplois de nos spécialistes, ce qui constitue une priorité pour cette famille professionnelle composée de civils comme de militaires.

En deuxième lieu, l'émergence d'un écosystème national propice. La cybersécurité est un domaine qui a besoin d'innovation et d'échanges, notamment entre les acteurs opérationnels et les acteurs de la base industrielle et technologique de défense, voire au-delà. La défense nationale y contribue par plusieurs initiatives, avec en particulier l'émergence d'un pôle d'excellence en matière de formation de Brest à Rennes, la mise en place d'une chaire de cyberdéfense à Saint-Cyr Coëtquidan ou un projet de pôle « cyber » du monde maritime sur la place de Brest.

En troisième lieu, la promotion d'une hygiène cybernétique implacable Aujourd'hui, nous constatons que sommes loin du compte et que les maillons faibles se trouvent en réalité chez nos grands partenaires. Cette hygiène repose sur une sensibilisation régulière, notamment dans toutes les formations internes, sur une information régulière du niveau de menace, qui permet de rappeler les bonnes pratiques, et sur des contrôles a posteriori tels que l'analyse après incident.

Enfin, la sensibilisation de la société aux enjeux cybernétiques tout en y développant l'esprit de défense. C'est toute l'ambition de la création d'une réserve citoyenne de cyberdéfense, dont Luc-François Salvador a accepté d'être le coordonnateur national, dans le cadre d'un engagement éthique et citoyen. Cette réserve citoyenne agit tant au profit de l'ANSSI que des armées et pourrait devenir apte à contribuer au traitement d'une crise informatique majeure sur le territoire national.

En conclusion, le ministère de la défense s'attelle à relever les enjeux de la cybersécurité par la mise en œuvre déterminée d'une vision directrice à dix ans. Les défis sont nombreux mais les acteurs civils ou militaires sont motivés et les relèveront.

Débat

M. le président Jean-Louis Carrère. J'invite maintenant les parlementaires et les personnalités présentes dans la salle à poser leurs questions.

M. Stanislas Bourdeaut (Alcatel-Lucent). Je remercie les intervenants d'avoir montré combien la cybersécurité est fondamentale pour la souveraineté

nationale. Ce sujet est au cœur des préoccupations des équipes d'Alcatel-Lucent en France.

Quelle influence peut avoir l'ANSSI sur les opérateurs privés qui se sont développés dans notre pays ? Ses recommandations sont-elles écoutées ?

Si l'idée d'édicter des normes européennes est intéressante, ne risque-t-on pas toutefois d'assister à un alignement sur le moins-disant ?

Alors que le rapport de M. Bockel préconise à juste titre que l'on retranche des cœurs de réseau les équipements malveillants, notamment chinois, où en est la réflexion sur l'accès ? Le plan télécoms du Gouvernement vise à étendre le très haut débit à la fois aux fixes et aux mobiles. La norme de quatrième génération reposant essentiellement sur des protocoles Internet tout aussi exposés que les cœurs de réseau, ne conviendrait-il pas de réfléchir à des mesures de prévention ?

M. Patrick Pailloux. En matière de normes européennes, le risque d'alignement sur le moins-disant est clairement identifié. La France joue ici un rôle d'explication et d'influence – j'ai même eu des échanges un peu difficiles avec la Commission européenne à ce sujet. Cela étant, je ne m'inquiète pas plus que de raison. Le sujet est bien identifié à l'échelle européenne, où l'on privilégie une stratégie de *capacity building*. Tous les État ne connaissent pas la même avance technologique, et de surcroît pas dans les mêmes domaines. Aussi la politique européenne vise-t-elle à tirer vers le haut l'ensemble du dispositif afin qu'il ne reste pas de maillon faible. Il est en effet probable, du fait de notre forte interconnexion, que d'éventuels attaquants utiliseront ce maillon.

La France, me semble-t-il, a eu une influence positive sur différents aspects de la stratégie européenne de cybersécurité dévoilée la semaine dernière. Je pense que nous allons dans le bon sens.

L'influence de l'ANSSI sur les opérateurs passe d'abord par un travail de sensibilisation et d'explication. Après avoir été victime d'une attaque, un opérateur a généralement une vision sensiblement différente de la situation !

Notre influence passe aussi par une action de régulation. Le dispositif législatif et réglementaire issu du « paquet télécoms » nous donne désormais la capacité de mener des audits auprès des opérateurs de télécommunication et de leur imposer des règles de sécurité. La question se pose toutefois pour les autres types d'opérateur.

M. Jean-Marie Bockel, sénateur. Je redis ici mon soutien aux salariés et aux responsables d'Alcatel-Lucent France. Je les ai rencontrés à plusieurs reprises et ils savent que je suis à leurs côtés. J'ai longuement évoqué leur situation avec Mme Pellerin. Nous ne devons pas oublier le caractère mondial de cette très belle entreprise, certes, mais nous devons nous garder de toute naïveté et renforcer ses

chances. M. Montebourg est sensible à cet aspect : il nous faut protéger nos fleurons tout préservant leur capacité à être présents à l'international.

M. Patrice Laya, rédacteur du site Sécurité commune info et membre du Haut comité français pour la défense civile. J'attire votre attention sur la pénurie de ressources humaines. Les jeunes ingénieurs préfèrent s'orienter vers les nouveaux développements des mobiles. Une fois la crainte du bogue de l'an 2000 dissipée et le passage à l'euro accompli, les entreprises et les organisations se sont séparées de leurs ingénieurs système et réseau ancienne architecture. À l'approche de la soixantaine, ils se retrouvent sur le carreau. Ne conviendrait-il pas de mettre ces personnes à contribution ? Écrire des codes et faire de l'assemblage, c'est comme la natation : cela ne s'oublie pas !

M. Patrick Pailloux. Il y a manifestement un déficit de formation. D'après une estimation menée avec les industriels qui recrutent dans ce domaine, il apparaît que la formation des experts de sécurité ne correspond qu'à un quart de ce qui serait nécessaire. Nous nous employons donc à développer des filières de sécurité, avec notamment l'ouverture d'une école spécialisée dans la région de Coëtquidan. Les cursus que nous mettons en place concernent bien entendu les jeunes, mais ils peuvent aussi permettre la reconversion de personnes ayant travaillé dans les systèmes et les réseaux.

M. le président Jean-Louis Carrère. En faisant appel à ces personnes, on pourrait mettre en place des formes de tutorat comparables à celles que le Président de la République préconise.

M. Jean-Marie Bockel, sénateur. La filière a un potentiel de création de centaines de milliers d'emplois qualifiés. Au moment du choix de leur formation, les jeunes sont sensibles à la conjonction d'un volontarisme industriel français et européen et à l'effet de mode dont peut bénéficier l'activité en question.

M. Claude Kirchner, délégué général à la recherche et à la technologie de l'institut national de recherche en informatique et en automatique (INRIA). Ma question, qui s'adresse à MM. Pascal Chauve et Stéphane Grumbach, concerne les données.

Naguère, lorsque l'on voulait acquérir de l'information, il fallait aller la chercher dans un endroit protégé par divers moyens, y compris cryptographiques. Aujourd'hui, on dispose également de données publiques, largement disponibles, dont l'agrégation et l'analyse permettront d'acquérir des informations que leurs détenteurs ne connaissent pas eux-mêmes. On peut imaginer que Google en sait beaucoup plus sur le ministère français de la défense que le ministère lui-même sur un certain nombre d'éléments.

Comment abordez-vous cette vulnérabilité et quels sont les moyens d'y répondre ?

M. Pascal Chauve. L'habitude de l'administration est de marquer d'un grand coup de tampon rouge ses informations classifiées. Elle s'attache à identifier précisément ce qui relève de la protection du secret de la défense nationale, de manière à ce que ces informations ne se retrouvent pas dans la nature : la compromission d'un secret protégé est punie par le code pénal.

Mais il existe une autre information, diffuse, qui permet par recoupement d'en apprendre beaucoup sur une entreprise ou sur un ministère comme par exemple le ministère de la défense, sur ses priorités, voire sur ses services de renseignement. Aucun coup de tampon ne peut résoudre ce problème, alors que l'accès au *big data* et à son traitement permet de dégager des informations précises. Pour remédier à cette situation préoccupante, il conviendrait sans doute d'étudier les technologies permettant de réaliser des recherches discrètes afin de dissimuler nos priorités. La discrétion des recherches, à laquelle l'INRIA travaille également, n'est pas qu'un sujet académique.

Pour le reste, nous ne disposons pas d'autre parade légale pour se protéger contre cette forme d'espionnage, que le régime de protection des données personnelles, qui ne s'applique dans le cas où de telles données, mélangées à des données de connexion ou, à des priorités de recherche, seraient compromises.

M. Stéphane Grumbach. Il faut en effet distinguer les données classifiées, les données personnelles accumulées par des industriels comme Google ou Facebook, et les données ouvertes – open data –, très populaires en Europe.

Les sociétés que j'ai citées sont propriétaires de leurs données. Dans la limite de certaines normes, elles peuvent en faire usage tant pour tirer des informations personnelles que des informations globales au niveau d'une région. On le voit, la situation est très différente selon que tous les pays possèdent ces informations ou seulement certains. En l'occurrence, les données de l'Europe ne sont pas en Europe, si bien que nous ne pouvons pas en faire grand-chose. Cela soulève un problème de souveraineté, y compris concernant les informations sur l'état de notre pays.

Pour autant, les données produites en France transitent par des tuyaux situés en France. De fait, elles pourraient être accessibles aux autorités françaises moyennant une analyse des paquets.

M. Jean-Yves Le Déaut, premier vice-président de l'OPECST. M. Pailloux pourrait-il apporter des précisions sur les mauvais résultats français en matière de tests de pénétration ?

Le capitaine de vaisseau Latty a pour sa part laissé entendre qu'il y avait des maillons faibles chez les grands partenaires du ministère de la défense. Peut-il en dire un peu plus ?

M. Patrick Pailloux. Les pirates informatiques entrant facilement dans les réseaux de nos grandes entreprises, il n'est pas étonnant que les tests de pénétration produisent les mêmes résultats. Pendant trente ou quarante ans, nous avons développé des systèmes d'information sans nous préoccuper véritablement de la sécurité. Le sujet dont nous débattons ici était encore, il y a deux ans, l'apanage de cercles très restreints. Les grandes entreprises et les grandes administrations ne s'en préoccupaient guère. De sorte qu'aujourd'hui nos systèmes d'information sont des portes ouvertes et les règles élémentaires d'hygiène informatique – auxquelles nous avons récemment consacré un guide – ne sont ni appliquées ni enseignées aux ingénieurs.

Que les audits de sécurité détectent des vulnérabilités est inquiétant mais n'est pas surprenant. Ce qui importe, c'est que leurs résultats soient bien pris en compte par la suite. Il nous arrive malheureusement de retrouver les mêmes vulnérabilités lors d'un test ultérieur !

M. le capitaine de vaisseau Alexis Latty. Il y a des maillons faibles partout, monsieur Le Déaut. Par contraste, nous estimons que les mesures prises au sein du ministère de la Défense nous ont mis sur la bonne voie. Mais nous avons de nombreuses interactions avec l'extérieur : fournisseurs de matériels, concepteurs ou,- développeurs de systèmes, et tous sont susceptibles de se glisser dans les « interstices » – comme les qualifiaient précédemment M. Chauve – de nos systèmes. Nous avons également des interactions avec des prestataires de services, en particulier de télémaintenance, qui disposent de points d'accès sur nos réseaux. Toutes ces interactions nécessitent la plus grande vigilance et que soit maîtrisé le niveau de cybersécurité des prestataires associés.

M. Daniel Kofman, professeur à Télécom ParisTech et membre du conseil scientifique de l'OPECST. Alors que l'on a évoqué à plusieurs reprises les problèmes pouvant se poser au niveau des cœurs de réseau, il me semble que les frontières du réseau présentent des vulnérabilités très importantes. Je veux parler des équipements personnels, tablettes et Smartphones, qui seront demain les passerelles entre notre réalité physique et le reste de l'infrastructure. Quelle est la réflexion des participants à ce sujet ?

On a peu évoqué également les algorithmes destinés à traiter les masses de données, les *big data*. À l'avenir, ces algorithmes apporteront des conseils directs aux citoyens. Pour l'heure, rien ne garantit qu'ils ne sont pas biaisés et répondent véritablement aux intérêts de ceux qui soulèvent les questions.

M. Patrick Pailloux. Les deux questions sont liées.

Le terminal personnel nous a fait changer de paradigme dans la mesure où la personne possède désormais un outil qui concentre la totalité de ses données : ses « contacts », ses messages électroniques, ses photos, sa localisation, ses accès à divers systèmes d'information. C'est donc un point de fragilité extrême en

termes de sécurité, d'autant plus faible qu'il est techniquement beaucoup moins puissant qu'un ordinateur.

En plus, les systèmes de ces terminaux sont contrôlés par un très petit nombre d'acteurs : essentiellement Google et Apple. Un client qui achète un mobile muni du système Androïd doit s'inscrire chez Google, sans quoi son équipement ne fonctionnera pas. De même, l'acheteur d'un e-pad, e-phone ou autre est contraint de s'inscrire chez Apple. Bien que le modèle soit ouvert d'un côté, fermé de l'autre, on doit de toute façon passer par ces sociétés pour accéder à la totalité de l'information. Ce sont elles qui gèrent votre identité et vos accès, qu'elles peuvent le cas échéant couper. Le sujet, rarement évoqué, pose de sérieux problèmes.

M. le président Jean-Louis Carrère. Auxquels s'ajoute celui de la dépendance à ces objets !

M. Eduardo Rihan Cypel, député. Nous abordons en réalité un nouveau continent qui recouvre tous les autres et où se joue non seulement la sécurité nationale – tout le monde s'accorde sur la nécessité de sécuriser les domaines vitaux –, mais aussi, ce dont on parle beaucoup moins, la vie concrète de nos concitoyens. De la sécurité nationale au petit appareil dont nous nous servons pour nous interconnecter, les enjeux sont imbriqués. Un des deux opérateurs cités va jusqu'à refuser de sécuriser les systèmes qu'il diffuse, sans doute par attachement à une conception « libertaire ». Mais comme toute la vie concrète passe par ces terminaux, les points de fragilité risquent de rendre vulnérables des systèmes beaucoup plus vastes. L'utilisation des comptes bancaires et de différentes données personnelles permet, par exemple, des activités d'intelligence économique.

Demain, ce seront les réfrigérateurs et tous les autres appareils domestiques qui seront interconnectés avec notre terminal. Nous pourrons tout contrôler à distance. Les ingénieurs prendront la relève des plombiers, qu'il ne sera même plus nécessaire de faire venir puisqu'ils pourront travailler à distance.

Le changement d'ère est encore plus important que celui qui a suivi l'apparition de l'automobile. Nous en sommes encore à une phase exploratoire qui devra s'accompagner d'une régulation forte, non pas pour contraindre les personnes mais pour organiser ce nouvel univers.

M. Michel Cosnard, président-directeur général de l'INRIA. Cette transformation de la société se traduit par une évolution de la notion de service public, puisque les questions dont nous parlons – défense nationale, mise en relation des citoyens, protection des données personnelles – relèvent bien du service public. La représentation nationale et l'OPECST réfléchissent-ils à cet aspect et à ses implications au regard de l'intérêt des citoyens ?

M. Bruno Sido, président de l'OPECST. Si j'ai souhaité l'organisation de ces tables rondes ouvertes au public et à la presse, c'est parce que jamais, dans mes douze années de mandat sénatorial où j'ai pourtant rapporté deux projets de loi relatifs aux télécommunications, je n'ai constaté que l'on ait vraiment abordé ces sujets, hormis peut-être à la commission de la défense et des forces armées. Les discussions d'aujourd'hui nous permettront de décider s'il est opportun que l'OPECST se saisisse de la question.

M. Jean-Yves Le Déaut, premier vice-président de l'OPECST. C'est à la suite d'auditions de l'INRIA que nous avons mesuré l'ampleur des problèmes, déjà abordés néanmoins par la commission de la défense et des forces armées de l'Assemblée nationale. L'OPECST a coutume d'être une passerelle entre le Parlement, le monde de l'université, le monde de la recherche et le monde industriel, mais c'est la première fois qu'il traite d'un sujet commun avec la défense. Les thèmes abordés ce matin ont des implications dans le domaine militaire. Cet après-midi, nous discuterons de leurs aspects civils.

Ces sujets majeurs pour notre pays relèvent bien, comme l'a dit M. Cosnard et comme l'ont bien démontré tous les intervenants, du service public. Nous devons nous en saisir. Se pose en particulier la question de la gouvernance mondiale de l'Internet. En dépit de quelques évolutions, le dispositif actuel, fondé sur des initiatives d'industriels américains privés, reste insatisfaisant. Au niveau national, les systèmes qui se mettent en place ont encore des progrès à faire.

M. le président Jean-Louis Carrère. Il me semble en effet que nous avons ici la première structure publique de débat sur ce thème. Et notre participation à des travaux qui requièrent une certaine confidentialité, quand ils ne sont pas soumis au Secret-défense, est assez récente. Nous n'avions pas l'habitude de ces préoccupations concernant nos téléphones mobiles, tablettes ou autres !

La Commission des affaires étrangères, de la défense et des forces armées du Sénat a travaillé à ces questions lors de la préparation de sa contribution au Livre blanc, il y a un peu plus d'un an. Auparavant, le rapport sur la cyberdéfense remis par Roger Romani en 2008 avait constitué une première parlementaire.

Je reconnais néanmoins que le Sénat s'en est tenu pour le moment à l'aspect de la cyberdéfense, sans explorer assez un autre aspect que je dois taire mais qui est indispensable. Comment, en effet, élaborer un dispositif de cyberdéfense avec des moyens seulement défensifs ?

Au sein de la commission du Livre blanc, le groupe de travail consacré au renseignement a beaucoup réfléchi à la cyberdéfense. Je crois ne trahir aucun secret en affirmant que ce sujet fera partie des priorités du document final.

Je remercie tous les intervenants pour la qualité de ces échanges.

II. DEUXIÈME TABLE RONDE : FIABILITÉ ET SÉCURITÉ NUMÉRIQUE DES SYSTÈMES D'ARMES

Présidence de M. Jean-Yves Le Déaut, premier vice-président de l'Opecst

Introduction par M. Jean-Yves Le Déaut, député, premier vice-président de l'OPECST

M. Jean-Yves Le Déaut, député, premier vice-président de l'OPECST, président. La première table ronde de la matinée visait à prendre la mesure de l'intensité des menaces induites par les attaques informatiques pour notre système de défense. Il s'agissait ainsi à proprement parler de la sécurité numérique. Cette seconde table ronde portera plutôt, quoique non exclusivement, sur la sûreté numérique.

Dans le domaine numérique comme, par exemple, dans le domaine nucléaire, la « sûreté » concerne les conditions du bon fonctionnement en soi et la garantie de réalisation de l'objectif par une mise en œuvre conforme à la conception, tandis que la « sécurité » concerne la résistance aux agressions volontaires externes et la capacité de continuer à fonctionner face aux attaques délibérées.

Permettez-moi d'illustrer cette différence avec un exemple tiré de l'actualité : dans le cas des lasagnes surgelées, la sûreté garantit que les barquettes mises en vente contiennent bien un mélange de pâtes et de viande de bœuf, tandis que la sécurité garantit que le produit est propre à la consommation. L'utilisation de viande de cheval est ainsi révélatrice d'une défaillance de sûreté du dispositif de production, mais pas à proprement parler d'une défaillance de sécurité.

Dans un monde devenu numérique, cette seconde table ronde vise donc à analyser les conditions permettant de garantir la sûreté des dispositifs numériques au cœur des systèmes d'armes comme des systèmes civils. La sûreté de la fabrication des systèmes numériques comporte, pour l'essentiel, une part qui n'est pas spécifique au domaine de l'armement. Dans tous les domaines en effet il faut modéliser, simuler et calculer le futur. Cet impératif se traduit par une préoccupation de qualité qui est commune aux secteurs civil et militaire : un système de pilotage automatique doit faire l'objet d'un contrôle très poussé, qu'il soit destiné au cockpit d'un avion de ligne ou à la tête de guidage d'un drone.

Je souhaiterais cependant que nos échanges d'aujourd'hui puissent montrer dans quelle mesure les technologies numériques sont effectivement duales, c'est à dire s'appliquent indifféremment aux domaines civil et militaire. En tant que nouveau membre de la Commission de la défense et rapporteur de l'avis budgétaire sur la prospective de la politique de défense, je suis en effet amené à m'interroger directement sur les conditions dans lesquelles des solutions du marché peuvent suffire pour répondre à des besoins liés à certains composants d'armement. Quelle recherche duale faut-il susciter ? Comment s'explique la carence de formation et comment y remédier ?

On peut se demander s'il n'existe pas des contrôles supplémentaires touchant en fait plus à la sécurité qu'à la sûreté et visant à repérer des capteurs espions ou des trappes aménagées intentionnellement afin de surveiller ou manipuler ultérieurement les systèmes une fois qu'ils sont en opération. Qui doit, en outre, gérer ces trappes si elles existent ?

Pour ce qui est de l'interconnexion des systèmes, la question de l'arbitrage entre gain et risque se pose pour des systèmes militaires comme pour des systèmes civils, tels les outils dématérialisés de transaction bancaire. Dans le cas des activités bancaires et financières, l'arbitrage a conduit manifestement à choisir le développement des interconnexions. N'y a-t-il pas des dimensions spécifiques à prendre en compte pour les interconnexions dans le monde militaire et les problèmes d'arbitrage ainsi soulevés ne sont-ils pas alors des vieux problèmes, déjà rencontrés face aux possibilités offertes par des formes plus anciennes de réseaux – notamment routiers ou ferrés ? Comment les systèmes d'information des différentes armées communiquent-ils ? Les faire communiquer présente-t-il plus d'avantages que de risques ?

On sent bien, intuitivement, que la multiplication des interconnexions apporte des gains d'efficacité pour la conduite des opérations, mais qu'en même temps elle rend les centres névralgiques plus directement vulnérables si l'ennemi parvient à pénétrer dans le réseau. Quelles sont les évolutions prévues ?

Quels sont les liens avec les milieux académiques ? Quelle recherche en SSI le ministère de la défense et la DGA promeuvent-ils ? Est-ce suffisant ?

Enfin, alors que la Direction générale de la sécurité extérieure (DGSE) et la Direction du renseignement militaire soulignaient hier devant la commission de la défense l'importance du traitement des informations, disposons-nous de systèmes suffisants en la matière ?

Avec plus de 1016 opérations à virgule flottante par seconde, la vitesse des calculateurs dépasse aujourd'hui le pétaflops. Combien en coûtera-t-il d'atteindre le chiffre de 1021 ? Les meilleurs seront-ils demain ceux qui possèdent les systèmes de calcul les plus puissants ?

Nous allons maintenant entendre M. Didier Brugère, directeur des relations institutionnelles et de l'intelligence économique du groupe Thales – lequel doit veiller à préserver tout au long de la chaîne industrielle, de la conception à la finition, la qualité et la sécurité des produits qu'il livre, notamment pour ce qui concerne les systèmes numériques qu'intègrent ces produits.

M. Didier Brugère, directeur des relations institutionnelles et de l'intelligence économique, Thales. Je commencerai par une anecdote : voilà environ vingt ans, l'entité que je dirigeais avait livré à l'un de nos clients militaires un système opérationnel embarqué qui, pour des raisons de coût, utilisait de la micro-électronique civile. En examinant l'un de ces équipements qui nous avait été retourné à la suite d'une panne, nous avons constaté qu'il était infesté par un virus. Plus surprenant encore : des jeux électroniques avaient été intégrés dans le système. Après enquête menée avec l'utilisateur, il est apparu que l'un des opérateurs, utilisant le lecteur de disquettes du système civil, avait introduit des jeux récupérés auprès de ses enfants et dont l'un était piraté et porteur d'un virus.

La première leçon de cette anecdote est que les problématiques que nous rencontrons aujourd'hui ne datent pas d'hier. Ce qui est nouveau, c'est la prise de conscience de l'importance et du danger de cette menace.

La deuxième leçon est que la vulnérabilité des systèmes de défense vient souvent de l'emploi des technologies civiles, bien connues et largement ouvertes et interconnectées. Cet emploi appelle certaines précautions.

La troisième est qu'il ne faut pas agir seulement au stade de la conception ou du développement d'un système, mais tout au long du cycle de vie des équipements.

Pour ce qui concerne le premier point, les industriels, dont Thales, s'emploient depuis des années à développer et intégrer des savoir-faire liés à la sécurité. Thales travaille ainsi depuis des décennies sur le chiffrement et la cryptographie et le fait que nous employions environ 1 500 ingénieurs dans ce domaine est le résultat de ces travaux engagés de longue date.

Pour ce qui concerne le deuxième point, les performances croissantes des systèmes d'armes tiennent à l'utilisation croissante des capacités de l'informatique, issues du monde civil et appliquées à des systèmes de défense. Pour bénéficier de l'apport de ces technologies numériques tout en assurant fiabilité et sécurité, il faut établir entre l'ensemble des intervenants des processus de développement – grandes entreprises, PME-PMI, services officiels et utilisateurs – une chaîne de confiance, un écosystème industriel qui s'inscrira dans la durée – c'est-à-dire parfois sur dix ou vingt ans, voire trente.

Cela suppose toujours une forte dimension nationale, car les enjeux relèvent de la souveraineté nationale. Une ouverture européenne est souhaitable et possible, mais elle est encore limitée.

Cela suppose aussi la maîtrise de certaines technologies critiques et des moyens de production associés. Ainsi, notre maîtrise des technologies et des savoir-faire en matière de chiffrement et de cryptographie nous assure une pleine indépendance sur ce terrain. Si nous sommes leaders dans ce domaine, c'est parce que l'État a investi depuis de nombreuses années dans l'industriel national spécialiste du chiffrement.

Cela suppose également la conception et la réalisation de composants électroniques. Si nous avons mis en place avec EADS une filiale commune pour les composants hyperfréquence – UMS – et racheté récemment la petite société allemande SYSGO, qui développe des systèmes d'exploitation à haut niveau de fiabilité et de sécurité, c'est pour pouvoir garder en France ou en Europe la maîtrise de ces technologies.

Cela suppose encore le développement de champions nationaux. Je ne reviendrai pas sur ce point, qui a été évoqué tout à l'heure, mais il faut mettre en œuvre une véritable politique industrielle dans ce domaine.

Cela suppose enfin le développement d'expertises très pointues, c'est-à-dire la mobilisation et l'entretien de tout un ensemble d'acteurs dans le domaine de la formation et de la recherche. En soutenant des chaires consacrées aux systèmes complexes à l'École Polytechnique ou sur la cybersécurité à Saint-Cyr, Thales contribue à développer cet écosystème.

Quant à la troisième leçon, selon laquelle tout ne se règle pas dès la conception et qu'il faut être capable de surveiller et de garantir la fiabilité et la sécurité du système tout au long de sa durée de vie, elle suppose la mise en place de mécanismes de surveillance et de détection en temps réel de l'intégrité des processus. Être en mesure de proposer de tels dispositifs est pour Thales un important axe de recherche.

Il faut pour cela une grande coopération entre l'ensemble des acteurs, notamment entre le fournisseur et l'utilisateur. Cette relation exige un partenariat de confiance fondé sur l'acceptation par les industriels de contraintes et d'engagements. Le ministère de la défense et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ont en la matière un rôle à jouer.

Une approche globale au niveau des systèmes, la maîtrise des technologies critiques, l'investissement dans la recherche et la formation, la surveillance continue des processus et la notion de partenaires de confiance sont, pour conclure, les concepts clés qui doivent guider notre approche de la fiabilité et de la sécurité des systèmes de défense face aux cyber-menaces.

Ces domaines dépassent le cadre des seuls systèmes de défense et touchent l'ensemble des systèmes d'information critiques que l'on retrouve aussi bien dans l'aéronautique que dans le secteur de l'espace ou dans les infrastructures de transports et d'énergie. Ce que nous faisons dans le domaine de la défense trouve très naturellement à s'appliquer dans les autres domaines. Thales, dont les activités relèvent pour moitié de la défense et pour moitié du domaine civil, s'attache donc à développer cette capacité à maîtriser les systèmes d'information critiques, qui conditionne la mutualisation des efforts et des investissements et rend la charge du développement des savoir-faire et des technologies supportable pour nos clients et pour nos propres capacités d'investissement. Cette mutualisation et cette approche globale des systèmes de souveraineté doivent nous permettre de rester leader en matière de maîtrise de la cyber-sécurité des grands systèmes.

M. Jean-Yves Le Déaut, président. Je vais donner maintenant la parole à M. François Terrier, chef du département ingénierie des systèmes et logiciels au laboratoire d'intégration des systèmes et des technologies du Commissariat à l'énergie atomique (CEA).

Monsieur Terrier, vous n'êtes pas directement en prise avec la production d'armes et nous ne sommes d'ailleurs pas ici pour chercher à dévoiler des secrets stratégiques. En revanche, vous semblez bien placé pour essayer de nous faire comprendre, à partir d'exemples tirés de ces outils délicats à mettre au point que sont les armes, quels sont les enjeux, en termes de fiabilité et de sécurité, de la fabrication de systèmes comportant un cœur numérique. Peut-être pourrez-vous préciser au passage les précautions supplémentaires imposées par le métier de l'intégration des systèmes dans l'univers militaire.

M. François Terrier, chef du département ingénierie des systèmes et logiciels au laboratoire d'intégration des systèmes et des technologies du Commissariat à l'énergie atomique. La volonté d'embarquer de plus en plus d'intelligence dans divers objets se traduit par des fonctionnalités de plus en plus riches, par une certaine complexité et par la nécessité d'interconnexions, de communication et d'ouverture. Des systèmes embarqués ne peuvent être figés d'emblée et ils doivent pouvoir s'adapter à un environnement changeant. Compte tenu de la complexité que cela suppose, des défaillances de sûreté sont possibles, et des portes permettent les interventions d'un système extérieur, comme cela a été identifié pour des réseaux électriques. Des objets courants peuvent ainsi devenir accessibles à des attaques, comme les réseaux de distribution d'énergie ou les réseaux routiers, ainsi que les systèmes automobiles. L'un des enjeux est donc la mise en place d'une ingénierie système et logicielle permettant d'analyser tout au long du processus les différents éléments à valider et certifier pour que le système soit correct.

Il s'agit donc d'un enjeu à la fois économique, lié à la qualité du produit, et de défense, lié à la mise en danger du territoire.

Ce développement de nouvelles techniques s'accompagne de la conscience que les systèmes sont développés par briques et qu'ils sont approvisionnés par des éléments provenant d'un marché très divers et ouvert, à propos duquel on ne dispose pas de tous les éléments d'information. Il est donc essentiel de pouvoir certifier ces éléments et d'intégrer cette certification dans la démonstration de sûreté ou de sécurité de l'ensemble du système. À cet égard, les normes sont des éléments structurants de la mise en place des processus de certification.

Il conviendra également de développer de nouveaux outils technologiques. Le CEA a développé des outils et des expertises permettant de concevoir des architectures de systèmes sûrs et de réaliser des analyses de sûreté de systèmes – liés certes au nucléaire, mais aussi à des domaines tels que l'avionique et l'automobile – avec des exigences variables en fonction des domaines. Nous tenons compte du besoin d'adapter ces outils en vue de la sécurité, compte tenu notamment du fait que les techniques formelles que nous utilisons pour l'analyse de sûreté d'un système pourront être déployées et adaptées pour réaliser des analyses de sécurité des logiciels embarqués dans ces systèmes. Cela supposera des recherches complémentaires, mais les bases de cette démarche sont bien structurées et très prometteuses.

La recherche et développement basée sur des techniques informatiques formelles progresse également au niveau européen, avec des projets importants regroupant de nombreux acteurs de la recherche et de l'industrie. Une conférence a d'ailleurs été organisée au début de la semaine sur le « e-government », c'est-à-dire les services en ligne destinés aux États, et les problèmes de sécurité correspondants.

Il importe donc de soutenir les techniques de développement et les chaînes d'outils utilisées pour développer les logiciels, afin de les adapter pour assurer un suivi de la sûreté de systèmes de plus en plus complexes en veillant à l'adaptabilité et à la reconfiguration des systèmes. Il convient également de prendre en compte le volet sécurité, qui présente des caractéristiques et des propriétés complémentaires à celles de la sûreté. Certaines technologies sur lesquelles travaille le CEA ont été développées en collaboration avec d'autres acteurs académiques, dont l'INRIA. Cet axe de travail est appelé à croître au cours des prochaines années.

M. Jean-Yves Le Déaut, président. Monsieur Jean-François Ripoche, vous êtes ingénieur en chef de l'armement et remplissez au sein de la Direction de la stratégie de la Direction générale de l'armement (DGA) la fonction un peu énigmatique d'architecte « Commandement et maîtrise de l'information ». Après nous avoir précisé la nature de vos responsabilités, vous voudrez bien aborder le sujet du deuxième thème de cette table ronde, qui consiste à faire le point sur

l'arbitrage entre les gains et les risques de l'interconnexion des systèmes numériques en matière d'armement.

M. Jean-François Ripoche, ingénieur en chef de l'armement. L'intitulé complet de ma fonction est le suivant : « architecte du système de forces 'commandement et maîtrise de l'information' ». Je suis chargé, conjointement avec l'État-major des armées, de préparer les programmes du futur pour les aspects liés à l'équipement, en matière notamment de recherche et de technologie, incluant les études amont. Il s'agit donc de l'amont des programmes d'armement.

Après les interventions que nous avons entendues, il ne fait aucun doute qu'un risque existe. Les deux précédents exposés, qui ont évoqué la fiabilité et la sécurité dans toute la filière de production des équipements, ont fait apparaître qu'il existait un champ de solutions concrètes, mais que des points clés devaient être surveillés – nous disposons de chiffreurs du meilleur niveau, mais cela ne suffit pas.

Pour ce qui est du gain, l'interconnexion des systèmes de défense est aujourd'hui un fait et une nécessité qui répond à des impératifs militaires. Il nous faut mieux connaître l'environnement dans le cadre des opérations – position des amis, des ennemis et des neutres, géographie, géolocalisation, météo… Les opérations peuvent être menées très vite, comme l'illustre la réactivité qu'il a fallu avoir pour l'opération Serval. Nos systèmes d'armes doivent être aussi efficaces que possible, face par exemple à la loi du nombre ou dans un cadre asymétrique, et leurs effets doivent être totalement maîtrisés, en termes de précision des cibles et d'effets collatéraux. Pour améliorer le temps de traitement des cibles par exemple, il faut accélérer le cycle du renseignement – orientation des capteurs pour savoir où regarder à grandes mailles, détection de points d'intérêt, analyse et action. Devant un ennemi furtif et très mobile, qui se déplace en pick-up et peut se cacher dans des grottes, il faut aller très vite et la réduction du délai séparant la constatation d'un indice d'activité et le traitement de la cible passe nécessairement par l'interconnexion.

Nous adoptons donc une posture de gestion du risque et une approche globale. Dans le monde de la défense, la notion de « systèmes d'information » ne se limite pas aux systèmes d'information opérationnelle informatiques à base de support tels que les messageries, mais elle englobe aussi les systèmes d'armes et les systèmes industriels qui peuvent se trouver dans leur environnement. Dans cette approche globale, les moyens de défense en complément des moyens de protection sont très importants. La maîtrise nationale de certains éléments clés du système est primordiale. Elle doit être étendue, au-delà des composants, à des briques logicielles ou à des plateformes de ce domaine. Il est également primordial de connaître l'état de la menace cybernétique.

J'en viens à l'arbitrage entre gain et risque. 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, comme l'automate de propulsion pour les navires et les chaînes de mobilité des blindés, dérivées du monde du camion, sans parler des systèmes d'information dans l'acception traditionnelle du terme.

La dualité est une opportunité, car le monde civil développe lui aussi de nombreuses protections qui peuvent nous servir, comme la biométrie permettant l'authentification des accès, les pare-feu sur les réseaux ou certaines messageries de niveau sensible.

En revanche, le monde civil s'est peu penché sur les hauts niveaux de sécurité, qui représentent un marché très étroit dans lequel la rentabilisation des efforts de recherche et de développement n'est pas assurée.

L'une des voies à suivre pourrait consister à utiliser ou encourager des initiatives européennes. Certains microprocesseurs, par exemple, pourraient être développés dans des filières européennes là où il n'existe que des filières asiatiques ou américaines.

Dans ses travaux axés sur la préparation de l'avenir, la DGA s'attache à mettre au point des architectures systèmes résilientes et prenant en compte à la fois les capacités de protection que nous pouvons intégrer et les vulnérabilités existantes. Ces architectures systèmes ne peuvent pas être universelles et doivent être adaptées à chaque cas et à chaque classe de cas : on ne protège pas un système d'information comme un système d'armes ou un système industriel – à quoi bon avoir un excellent chiffreur si la porte du local électrique est ouverte ?

Ces systèmes ne doivent pas seulement être protégés : il faut les rendre défendables, ce qui suppose de savoir comment ils sont construits et d'être capables d'analyser les flux de données. Il faut aussi les rendre résilients, ce qui pourrait passer par une forme de convergence entre la sûreté de fonctionnement et la sécurité assez prometteuse. Si une telle démarche avait été adoptée dès le début face à Stuxnet, peut-être y aurait-il eu la mise en place à la fois des dispositifs de protection et des dispositifs empêchant l'instrument de se mettre dans un mode de défaillance. Ces deux approches couplées sont potentiellement très intéressantes.

Le monde de la défense se caractérise par une grande hétérogénéité de ses systèmes d'armes. Un Rafale va durer plus de quarante ans, et l'on voit bien la différence entre l'informatique d'il y a quarante ans et celle d'aujourd'hui. Les nouveaux systèmes que nous développons tiennent compte dès le départ de l'impératif de sécurité informatique. Pour les systèmes existants, nous faisons au mieux, en évitant les maillons faibles. De simples mesures organisationnelles peuvent permettre d'atteindre à coûts mieux maîtrisés l'objectif d'une meilleure sécurité informatique.

Enfin, la question de l'interopérabilité avec nos alliés est très importante. Face à la multitude de systèmes en usage dans les différents pays et au sein de l'OTAN, seules les démarches pragmatiques ont un avenir. L'Afghan Mission Network, en Afghanistan, avait ainsi assez bien réussi à cantonner les problèmes de sécurité de l'information à certaines interfaces, avec des passerelles d'accès à des réseaux, l'OTAN défendant ses réseaux pendant que les nations défendaient les leurs.

Nous vivons dans un monde interconnecté, y compris pour la défense, avec un risque que nous nous efforçons de gérer au mieux. Cela nécessite un effort sur le plan des ressources humaines comme sur le plan financier. Le budget affecté aux études amont réalisées par la DGA devrait doubler en 2013 par rapport à 2012. La sélection des sujets que nous traitons se fait en étroite collaboration, voire en cofinancement, avec l'ANSSI, afin que l'ensemble de la communauté nationale puisse bénéficier de ces travaux.

M. Jean-Yves Le Déaut, président. Je vais maintenant donner la parole à M. Jean-Luc Moliner, qui va nous apporter l'éclairage qui procède de l'expérience d'un grand groupe international – Orange – en matière de gestion des risques liés à l'interconnexion des systèmes numériques. Pour avoir été antérieurement responsable de la sécurité des systèmes d'information à l'État-major des armées, M. Moliner a une parfaite connaissance des enjeux de la « guerre en réseau ». Il a également vécu récemment l'attaque qui a valu aux clients d'Orange une journée de gratuité.

M. Jean-Luc Moliner, directeur de la sécurité, Orange. La panne du 6 juillet 2012, qui a entraîné l'indisponibilité du réseau pendant 11 heures, n'était pas le résultat d'une attaque, mais le résultat d'une panne technique d'un élément essentiel de notre cœur de réseau.

Orange est à la fois un opérateur international présent dans plus de 170 pays à travers le monde, gérant un réseau d'interconnexions mondial, et un prestataire de services fournissant des réseaux fermés aux principaux services de l'État et des transmissions aux services de la défense aérienne ou de la coordination du trafic aérien. L'interconnexion est l'élément fondateur de l'explosion actuelle des télécommunications. C'est le moteur de la vie que connaîtront demain tous les citoyens.

Les interconnexions permettent aux individus un partage dynamique et fluide de l'information. N'importe où dans le monde, on peut aujourd'hui se connecter avec des délais de réponse inférieurs à quelques secondes, voire à la seconde. L'interconnexion est démultipliée par l'« Internet des objets ». Des millions d'objets sont déjà connectés à des réseaux intelligents. Demain, on en comptera des milliards. Cette déferlante est tournée vers l'optimisation des « réseaux intelligents » ou de la « ville intelligente ».

Cette évolution a des effets que certains peuvent juger pervers, comme la possibilité de savoir combien de personnes viennent d'entrer dans la maison ou quel est votre profil d'utilisation de certains services – eau, électricité ou chauffage, par exemple.

Le marché des télécommunications explose : on comptait chaque mois 600 millions de gigaoctet en 2011, puis 1 300 millions en 2012. Ce chiffre doublera en 2013, pour atteindre 10 800 millions de gigaoctet par mois en 2016. Cette quantité d'informations doit circuler d'une manière parfaitement fluide, avec des taux de disponibilité élevés.

La structuration des réseaux a pour objet de transférer des contenus, qui circulent entre des *data centers* entre l'Asie, l'Europe et les États-Unis, et de permettre à un utilisateur d'avoir accès à ces données. Les profils d'utilisation sont très variés. Ainsi, 10 % des clients d'Orange consomment 70 % de notre bande passante.

L'une des questions qui peuvent se poser aux armées est celle de savoir où dans le système se situe la puissance de calcul – près des données ou près des utilisateurs –, ce qui pose des problèmes d'architecture assez compliqués.

L'interconnexion provoque des problèmes de sécurité dans notre propre écosystème comme avec les écosystèmes avec lesquels nous pouvons être interconnectés.

Au-delà des questions de disponibilité, les problèmes intérieurs sont principalement dus au comportement des usagers. Nos clients ne sont pas sensibilisés à ces questions et tous les opérateurs de télécoms ont parmi leurs clients un pourcentage assez significatif de gens qui hébergent des réseaux de Botnet, malwares qui vont à leur tour attaquer d'autres systèmes.

En France, des réglementations nous empêchent d'avertir de manière proactive le client qu'il est infecté. Les attaques, quant à elles, sont massives. Ainsi, l'an dernier, des flux de données de 40 gigabits par seconde circulaient sur notre réseau en direction de quelques cibles, provoquant des effets collatéraux assez importants. Ces données provenaient du monde entier dans des attaques coordonnées. Nous savons gérer des attaques de ce type, mais elles perturbent profondément les réseaux pendant plusieurs heures et leur généralisation poserait à terme d'importants problèmes.

Nous sommes par ailleurs handicapés par l'industrie du logiciel. Le développement mal maîtrisé du langage Java, fourni par la société Oracle, est à l'origine de nombreuses failles installées chez tous les clients utilisant ce type de logiciels et nous ne disposons pas de normes ou de processus permettant de garantir que les logiciels, même destinés au grand public, présentent un niveau de

sécurité acceptable. Du reste, la diffusion de logiciels de mauvaise qualité ne cause aucun dommage à la société Oracle.

Des problèmes de filtrage se posent au niveau des frontières. Le monde des télécoms a en effet été imaginé par des gens bien élevés qui n'ont pas envisagé les attaques massives que nous connaissons et qui, pour nous, se traduisent principalement par de la fraude.

L'interconnexion des réseaux au profit des différentes armées ou du Gouvernement est un peu plus simple, car un réseau fermé d'abonnés permet un niveau de sécurité que la DGA ou le Secrétariat général de la défense nationale peuvent juger satisfaisant. En revanche, la sécurité des équipements de réseau pâtit d'un système relativement hétérogène, comprenant des matériels provenant d'une douzaine de fournisseurs dont les centres de développement et de fabrication sont établis principalement en Asie, y compris pour des sociétés américaines ou européennes. L'une des difficultés consiste donc à s'assurer que les équipements que nous sommes contraints d'acheter chez eux présentent un niveau de qualité suffisant. Faute de pouvoir vérifier toutes les lignes de code fournies, il nous faut assurer une gestion du risque sur le fonctionnement normal de certains événements. Qui plus est, les évolutions de ces logiciels sont relativement fréquentes, avec des paliers technologiques tous les six à neuf mois. Maintenir une infrastructure mondiale de télécoms qui soit à la fois intègre et disponible et qui puisse satisfaire l'ensemble des objectifs que nous nous sommes fixés est un véritable challenge.

L'interconnexion des systèmes d'information suppose, pour permettre la surveillance de nos propres systèmes, l'intégrité des informations qui remontent, afin d'éviter le déclenchement intempestif de systèmes automatiques d'autoprotection face aux attaques.

M. Jean-Yves Le Déaut, président. M. Christian Malis est professeur associé à Saint-Cyr Coëtquidan. Il a aujourd'hui pour tâche de montrer que les questions que nous nous posons à propos des enjeux stratégiques de l'interconnexion des moyens numériques modernes en termes d'avantages et de risques sont en fait des questions anciennes qui se sont déjà posées dans le passé lors d'avancées techniques intervenues dans les réseaux de communication au sens large, c'est-à-dire concernant aussi bien le transport des moyens militaires que le transport d'information.

M. Christian Malis, historien, professeur associé à Saint-Cyr Coëtquidan. Je m'exprimerai en tant que professeur d'histoire militaire à Saint-Cyr. Il se trouve que j'appartiens aussi à la société Thales, mais je tiens à préciser que ce n'est pas moi qui exprime aujourd'hui le point de vue de cette société.

Je vais m'efforcer de tirer brièvement de l'histoire de la guerre et de l’impact stratégique de certaines transformations techniques quelques éléments de jugement sur le problème qui nous préoccupe dans le cadre de cette table ronde.

La perspective de l'histoire est-elle légitime ? Le monde numérique interconnecté présente toutes les apparences de l’hypermodernité, mais il présente incontestablement aussi des équivalents historiques. Le cyberespace est une nouvelle infrastructure de transport d'informations dont les origines sont au moins partiellement militaires – si l’on fait d’ARPANET, le réseau américain de la DARPA, l’ancêtre de l’Internet – mais aussi un milieu social et une réalité géopolitique. En ce sens il peut être rapproché, à vingt siècles de distance, du réseau des voies stratégiques romaines, dont la construction s’est étalée sur quatre siècles et qui représentait un système véritablement dual : ces routes, qui devaient faciliter le passage des légions et des lourds convois d'artillerie avaient également une vocation économique pour la circulation des négociateurs et des biens, ce qui en a fait un outil de propagation de la civilisation romaine.

Sans remonter aussi loin, j’évoquerai maintenant la mise en place au xxe siècle et la succession d’infrastructures de transport et de communication qui ont modifié en profondeur la stratégie et la morphologie de la guerre : le réseau ferré et le réseau télégraphique pendant la Première Guerre mondiale, puis l’usage du réseau routier pour le déplacement des armées motorisées et blindées pendant la Deuxième Guerre mondiale et enfin le réseau stratégique de transport aérien américain mis en place lui aussi durant la Deuxième Guerre mondiale. Je m'efforcerai de présenter leur succession comme obéissant à une logique dialectique.

J’évoquerai d’abord la Première Guerre mondiale et les nouvelles infrastructures de la guerre industrielle.

L'historien israélien Martin Van Creveld a baptisé « âge des systèmes » la période de 1830 à 1845 du point de vue de la technologie militaire. Désormais, l’organisation s’applique à la technologie, et non plus seulement à des êtres humains. Les machines se trouvent intégrés dans des systèmes technologiques complexes qui assurent leur coordination.

L'infrastructure ferroviaire permet le déploiement stratégique, dans des délais raisonnables, d’armées nationales fortes de plusieurs centaines de milliers et même de plusieurs millions d'hommes.

Le réseau télégraphique joue un rôle important pour permettre le commandement et le contrôle de ces masses armées dispersées sur des centaines de kilomètres de front : au XVIIe siècle, l'extension des armées pouvait atteindre quelques kilomètres et, à l'époque de Napoléon, quelques dizaines de kilomètres seulement.

La stratégie défensive consiste à manœuvrer par le rail sur ses lignes intérieures pour colmater une brèche ou concentrer des troupes avant un assaut.

L'usage du réseau ferré et de plus en plus du réseau routier jouent donc un rôle très important dans la défensive finalement victorieuse de l'armée française, puis dans le retour final à une stratégie offensive victorieuse en 1918.

En deuxième lieu, j'évoquerai le Blitzkrieg et le contre-blitzkrieg : l'adversaire allemand réagit en exploitant à son profit le réseau routier pour restaurer la guerre de mouvement offensive, grâce à de nouvelles tactiques de pénétration à l'aide de divisions blindées, mais aussi en exploitant la jeune arme aérienne au profit d'une action dans la profondeur : l'aviation de bombardement allemande sert, en Pologne puis en France, non seulement à appuyer les troupes à l'assaut, mais d'abord à détruire au sol l'armée de l'air adverse et à détruire les gares de triage, les ponts, et les concentration de troupes. Par ailleurs l'armée allemande protège ses colonnes motorisées et blindées – la percée de Sedan a été précédée de 150 kilomètres d'embouteillages – des raids aériens français par un usage beaucoup plus intensif de l'armement anti-aérien.

Selon l'image employée plus tard par le stratège britannique J.F.C. Fuller, l'armée française a été battue en 1940 parce qu'elle a opposé une défense statique et linéaire du type de celle de 1914-1918 à des modes nouveaux d'attaque par pénétration, un peu comme un homme qui voudrait barrer la route à un boxeur en étendant les bras. Il aurait fallu concevoir une défense échelonnée dans la profondeur et manœuvrante, ainsi décrite par un chroniqueur militaire de l'époque, Stanislas Szymonzyk : « comme toute manœuvre de la guerre moderne, la retraite employée comme méthode stratégique suppose une préparation minutieuse : destructions de toutes espèces par des unités spéciales, procédés anti-tanks (mines, fossés, barrages...), organisation du pays ; le réseau routier, splendide, de la France, aurait dû être utilisé pour les manœuvres de la défense élastique et non pour l'évacuation des populations ». Les Soviétiques, par doctrine et parce qu'ils disposaient d'une plus grande profondeur territoriale, ont su déployer une telle défense dans la profondeur.

J'évoquerai enfin le transport aérien militaire américain pendant la Deuxième Guerre mondiale. La conduite américaine de la guerre s'appuie – c'est peu connu – sur l'exploitation industrielle d'une nouvelle profondeur stratégique : le milieu aérien en vue du déplacement des troupes, du matériel et de l'aviation de bombardement à l'échelle intercontinentale.

L'Air Transport Command dispose très vite d'un réseau qui s'étend aux cinq continents. Les quadrimoteurs venus des États-Unis se ravitaillent à Marrakech, devenu une plaque tournante, avant de rejoindre le Moyen-Orient, d'autres escadres y font escale avant d'aller bombarder l'ennemi en Tripolitaine, en Italie ou en Roumanie, où se trouvent les installations pétrolières de Ploesti. Des « facilités » nouvelles – ateliers d'entretien technique, parcs automobiles et

cantonnements – et toute l'infrastructure du contrôle aérien moderne sont mises en place. Cette maîtrise technique et industrielle n'apparaît pas seulement dans la maîtrise générale des flux et dans la recherche générale du rendement qui contraste avec la médiocre productivité qui avait caractérisé la France, son industrie et une partie de ses activités militaires dans les années 1930, mais aussi dans un degré élevé de spécialisation des métiers de l'Air – notamment contrôleurs aériens, mécaniciens, radios, météorologistes et manipulateurs de cargo. Derrière la pointe aérienne combattante il y a donc toute une ressource spécialisée pour servir cette vaste infrastructure.

Ce sont ces progrès dans l'industrialisation du transport qui ont permis le fantastique développement de l'aviation civile après la Deuxième Guerre mondiale.

Je conclurai par quatre éléments de jugement.

Tout d'abord, la sanctuarisation totale du dispositif numérique étant impossible, il faut prévoir une défense opérationnelle dans la profondeur, par opposition à une défense périmétrique et statique. Sa version contemporaine comporte deux volets. Le premier est celui de la sécurité native dans la conception des systèmes d'armes et informatiques embarqués, des systèmes d'information et de communication, des systèmes industriels, des drones et des autres types de robots militaires. Le deuxième volet est celui de la protection, jusqu'au niveau de la donnée, dans les systèmes d'information publics ou privés. Dans cet esprit, je ne crois guère à des forces armées capables de fonctionner durablement en mode dégradé, c’est-à-dire susceptibles de s’affranchir du recours aux systèmes numériques dans un contexte de blitz cybernétique, sinon en cas de défaillances locales et temporaires. De fait, on n’a jamais désappris un nouveau mode de fonctionnement technologique et ce mode dégradé est difficile à concevoir comme mode structurel de fonctionnement des forces armées.

Ensuite, depuis la Deuxième Guerre mondiale, la profondeur industrielle et technique, qui représente en soi une forme de profondeur stratégique, est un préalable critique pour tirer pleinement parti de l’interconnexion des systèmes numériques et en dominer les risques. Dans le domaine de la cyberdéfense, la sûreté et la sécurité dans la durée dépendront de la capacité à mettre en place une force humaine et industrielle de grande envergure.

En troisième lieu, la stratégie est affectée d’une logique paradoxale : on a affaire à un adversaire intelligent. En 1940, la Wehrmacht recherche la surprise déstabilisante – « the line of least expectation », ou le contrepied. Or, la « cyber » est par excellence le domaine de l'imagination, de la prolifération technique et de la créativité, et cela d’autant plus que le ticket d'entrée est peu élevé.

Je conclurai donc en citant Churchill : « Aussi légitime soit-il pour le haut commandement de se préoccuper de sa propre doctrine, il est parfois utile de

s’intéresser à celle de l’ennemi ». On devrait s’interroger sur le motif, l’intention stratégique d’un adversaire recherchant ou provoquant une agression cybernétique de grande envergure. Ce motif ne serait-il pas avant tout psychologique, ayant un rapport avec le lien d’obéissance et de confiance qui relie les populations à l’autorité politique. L’affaire Al Chamoun devrait être méditée, mais des précédents existent, durant la Deuxième Guerre mondiale comme au Moyen Âge – mais c’est là un autre sujet que je réserve à l’éventuelle discussion que nous aurons tout à l’heure.

M. Jean-Yves Le Déaut, président. Merci pour cet exposé qui donne un ancrage historique aux problèmes contemporains.

Débat

M. Claude Kirchner. Monsieur Moliner, La panne du 6 juillet 2012 relevait-elle de la sécurité ou de la sûreté ? Quels ont été les effets collatéraux, en interne comme en externe ?

M. Jean-Luc Moliner. Cette panne a atteint le cœur de réseau, et plus précisément le HLR (Home Location register) qui permet d’authentifier et de localiser les utilisateurs de téléphones mobiles lorsqu’ils sont connectés. Des analyses ternes et externes ont relevé un certain nombre de dysfonctionnements consécutifs. La commission de sécurité de la Fédération française des télécoms, que je préside, ainsi qu’une association des opérateurs de télécoms européens, dont je suis membre, analysent aussi ces incidents majeurs. Une semaine après celui dont nous parlons, un autre du même type a eu lieu en Angleterre sur le réseau de la société Telefónica O2. Le groupe Telefónica avait d’ailleurs connu un problème similaire en Argentine.

Nous nous efforçons de tirer les enseignements de ces incidents récurrents et d’origines diverses, qu’il s’agisse de la conduite à tenir, du paramétrage ou de l’architecture globale. Ces échanges d’informations participent à la sécurisation de nos infrastructures.

M. Claude Kirchner. Qu’en est-il des effets collatéraux, notamment pour les utilisateurs ? Cette défaillance est en effet l’une des plus importantes subies par un réseau de téléphonie.

M. Jean-Luc Moliner. Seuls les utilisateurs en mouvement ont été concernés par la panne. Les leçons de cet événement ont été tirées, et des changements ont été apportés afin de sécuriser les infrastructures encore plus fortement qu’elles ne l’étaient. Pour information, nos « home location registers » (HLR) sont répartis en six lieux différents, et les bases de données sont multipliées par trois pour chacun des serveurs : cette configuration représente déjà ce qui, aujourd’hui, se fait de mieux sur le marché en termes de sécurité.

M. Frédéric Hannoyer. Les activités de ST Microelectronics étant essentiellement civiles, je ne suis pas un spécialiste des systèmes d'armes. Ma question est la suivante : qu'en est-il de la gestion du risque, notamment au regard de la pervasion des terminaux de grande consommation – y compris chez les militaires – et du rythme d'évolution de ces terminaux ? Les plateformes qui seront annoncées au congrès de Barcelone, la semaine prochaine, auront quatre cœurs à plus de 1 GHz, capacité très supérieure à celle dont disposait un ordinateur il y a quelques années. En ce domaine, les évolutions sont très rapides, et il faut aussi compter avec la consumérisation des logiciels. Certains applications, autrefois vendues plusieurs centaines ou milliers d'euros, le sont aujourd'hui pour deux euros seulement sur des appstores. La sécurité et la chaîne de valeur des outils n'en seront que plus difficiles à assurer. Finalement, les réseaux de défense sont fermés et relativement étanches ; cependant, existe-t-il des risques d'interpénétration de votre réseau par les réseaux de consumérisation qui les entourent, qu'il s'agisse des militaires sur le terrain – qui peuvent être connectés par leurs équipements personnels – ou par l'usage de clés de stockage – ou enfin par les réseaux domotiques des bâtiments militaires qui deviennent de plus en plus gérés comme des immeubles intelligents par des systèmes automatisés de capteurs communicants ?

M. Jean-François Ripoche. Les terminaux civils sont en effet de plus en plus performants : c'est là une évolution que nous sommes obligés de suivre. Les réseaux militaires utilisent des débits assez bas au regard de la norme Internet, ce qui présente des inconvénients mais aussi des avantages en termes de sécurité. Cependant, le grand progrès des terminaux récents est l'intuitivité, que nous voulons aussi retrouver dans nos systèmes d'armes. Nous pouvons par ailleurs utiliser un terminal civil en lui ajoutant des éléments matériels ou logiciels, afin de diminuer sa vulnérabilité. Enfin, n'oublions pas que la défense est par certains aspects une entreprise du secteur tertiaire, ce qui l'expose à une plus grande porosité dans ce cadre. Cela dit, un soldat sur le terrain n'a pas davantage le temps de se connecter à Internet avec son téléphone qu'un opérateur de n'importe quelle entreprise. Cela limite un peu les risques.

M. Didier Brugère. Dès lors que la menace est reconnue, on évalue son niveau et celui de la protection recherchée. Ce travail, qui permet aux industriels de proposer des solutions adaptées, doit se faire avec les utilisateurs et les services officiels ; d'où l'importance de la chaîne de confiance et du partenariat. En l'espace de quelques années, la menace a fait l'objet d'une vraie prise de conscience, dont le futur Livre blanc constituera le point d'orgue. L'ensemble du système et de ses opérateurs pourra alors se mettre en marche.

M. Michel Cosnard. Comme l'a observé M. Moliner, des milliards d'objets intelligents seront bientôt connectés. Dans l'aéronautique, les normes, traditionnelles, semblent avoir donné satisfaction ; dans le secteur bancaire, elles semblent plus drastiques mais restent globalement traditionnelles aussi. Qu'en est-

il pour les nouvelles applications, en particulier dans le domaine médical, du moins en dehors de la salle d'opération, où les normes sont bien moindres, comme le montre l'exemple des pacemakers ? Des problèmes sont aussi apparus sur les systèmes embarqués dans les automobiles. Des travaux et des réflexions sont-ils menés au niveau européen ?

M. François Terrier. Ces questions sont difficiles, mais elles représentent un enjeu réel. L'absence de normes est un problème ; au demeurant, la définition de la juste norme est aussi un enjeu industriel. Quoi qu'il en soit, des réflexions sont en cours sur les smart grids, afin de définir des normes qui garantissent leur sécurité sans générer des coûts de démonstration intenables. La recherche d'un tel équilibre fait la spécificité de l'Internet des objets par rapport à l'aéronautique ou au nucléaire, même si celui-ci, faisant face à l'internationalisation des normes, doit en permanence réfléchir à la façon d'y adapter ses systèmes sans les changer de fond en comble. En tout état de cause, des projets sont en cours, qu'il faut encourager et développer au niveau des pouvoirs publics, des acteurs industriels comme de la recherche, laquelle peut contribuer à trouver des solutions performantes à des coûts maîtrisés.

M. Jean-Luc Moliner. L'une des grandes questions actuelles, pour les télécoms, est la dématérialisation des cartes SIM, qui en France font l'objet d'une certification EAL 4+ par l'ANSSI, soit le niveau de sécurité le plus élevé. En matière d'Internet des objets, les industriels ont tendance à vouloir noyer les fonctionnalités dans le silicium, sans garantie de sécurité. Les débats, au sein d'organismes de normalisation européens et internationaux, portent donc essentiellement sur les risques de fraude ; leur teneur est critique car, en France et en Europe, ces questions concernent toute une filière industrielle de compétences.

M. Jean-Yves Le Déaut, président. J'exprimerai un point de vue de parlementaire. On a beaucoup évoqué la dualité entre la recherche civile et militaire, ainsi que les exigences de haute sécurité, notamment pour les laboratoires de type P4, ceux de l'INRIA et ceux de la DGA d'une part et de l'État-major des armées de l'autre, au sein desquels on étudie des virus particulièrement dangereux. J'ai eu l'occasion de visiter le laboratoire civil, et ne tarderai pas à visiter le laboratoire militaire. Les liens entre les deux vous paraissent-ils suffisants ? Des relations plus étroites ne permettraient-elles pas de développer la formation ? Plus généralement, les relations entre le civil et le militaire dans le domaine de la haute sécurité des systèmes informatiques vous semblent-elles suffisantes ?

M. Claude Kirchner. Le laboratoire de haute sécurité informatique, installé dans le centre de recherche de Nancy, collecte virus et malwares afin de les analyser et de tester la résistance de nouveaux logiciels. Bien qu'ils existent déjà, les liens avec la DGA mériteraient d'être renforcés, d'autant que certaines

compétences apparaissent complémentaires. Il convient aussi d'améliorer la formation des personnels susceptibles de travailler dans nos laboratoires.

M. Jean-François Ripoche. La DGA souhaite rester en relation avec la recherche académique, que ce soit, par exemple, à travers l'INRIA de Nancy ou les écoles normales supérieures de Cachan et de la rue d'Ulm, où sont menées des recherches sur la cryptographie. Beaucoup de contractuels employés par la défense ont aussi vocation à rejoindre l'industrie ou d'autres administrations, où ils pourront diffuser leurs acquis. Nous souhaitons tous intensifier les efforts, ce qui passe par une augmentation des échanges. Je rappelle que le centre d'excellence de la DGA est la DGA-MI, à Bruz, non loin de Rennes.

M. Didier Brugère. Le partage de l'effort de recherche concerne aussi les industriels. On constate, depuis plusieurs années, un renforcement des liens entre la recherche étatique et la recherche industrielle. Ont ainsi été créées des unités telles que le laboratoire commun entre Alcatel-Lucent, le CEA-Leti et Thales, ou celui créé en partenariat avec le CNRS, respectivement spécialisés dans les technologies de composants très avancées et les technologies de magnétorésistance. Sur des sujets qui intéressent aussi bien le civil que le militaire, de tels rapprochements doivent être poursuivis et encouragés car ils sont essentiels pour l'avenir.

M. Jean-Yves Le Déaut, président. J'aborde ce point dans le rapport consacré à la traduction législative des Assises de l'enseignement supérieur et de la recherche que je viens de remettre au Premier ministre. Une telle dualité est assez emblématique de la situation française, même s'il ne faut pas la généraliser. Entre les écoles d'ingénieur et les universités, les cultures demeurent malgré tout différentes. La seule question de la reconnaissance du doctorat montre toute la difficulté qu'il y a à traiter avec chacun des corps. Le niveau de coopération entre le civil et le militaire n'est pas optimal, ce qui pénalise notre pays par rapport à d'autres, comme les États-Unis, où les deux types de recherche sont totalement intégrés. J'aurai l'occasion d'y revenir dans le cadre des travaux qui prolongeront mon rapport.

M. Bruno Sido, sénateur, président de l'OPECST. Les systèmes dont nous parlons sont extraordinairement fragiles, puisque chacun trouve normal que l'on y entre comme dans une motte de beurre. Une telle fragilité me semble être une régression. Vous êtes passé de la Rome antique à la Première guerre mondiale, monsieur Malis, et peut-être aurait-il fallu parler du Moyen Âge. Mais j'évoquerai pour ma part la Seconde guerre mondiale, au cours de laquelle le système de cryptage allemand Enigma n'a jamais pu être percé, jusqu'à ce que les Alliés mettent la main sur un sous-marin en train de couler. Que penser de la robustesse des systèmes d'alors, par comparaison avec la fragilité de ceux d'aujourd'hui ?

M. Christian Malis. Le percement d'Enigma est l'une des raisons cachées du retournement de situation en Afrique du Nord lors de la Seconde guerre mondiale. Par ailleurs, l'intention stratégique qui avait présidé au bombardement de l'Allemagne nuit et jour était, comme l'observait un stratège italien, de briser le lien entre les autorités et la population en lui montrant que celles-ci ne la protégeaient pas. Le but, en somme, était de provoquer une insurrection : au-delà de la destruction d'un potentiel de guerre, les bombardements stratégiques constituaient d'abord une arme subversive et psychologique. Les Allemands ont résisté grâce à une défense dans la profondeur, au sens le plus fort du terme, puisque 2 millions d'hommes étaient mobilisés pour reconstruire les infrastructures bombardées. Une défense dans la profondeur n'annule donc pas les risques : elle permet une résistance dans la durée.

M. Michel Cosnard. Seul l'appareil de cryptage d'Enigma avait été trouvé dans le sous-marin : les codes, eux, furent cassés par l'équipe d'Alan Turing, l'un des pères fondateurs de l'informatique. Ce décryptage, d'autant plus difficile que les codes changeaient en permanence, fut réalisé grâce aux plus gros calculateurs de l'époque, à l'origine de l'informatique. La maîtrise des « super-calculateurs », depuis leur conception jusqu'à leur utilisation, est en ce sens un enjeu majeur pour la défense nationale.

M. Jean-Yves Le Déaut, président. En quoi, monsieur Moliner, la législation vous empêche-t-elle d'avertir ceux de vos clients qui détiennent des malwares ? Quelles modifications faudrait-il apporter en ce domaine pour corriger ce qui peut l'être, dès lors que l'information est connue ?

M. Jean-Luc Moliner. La loi, qui protège la vie privée des clients, interdit aux opérateurs de télécoms d'analyser le trafic et d'avertir les clients individuellement. Nous ne pouvons donc mener que des études statistiques, sur la base de données anonymes.

M. Jean-Yves Le Déaut, président. Nous serions intéressés par une discussion et une analyse juridique du sujet, afin de trouver des solutions permettant de prévenir les attaques. L'incident subi par votre système n'était pas une attaque, mais il aurait évidemment des conséquences très graves s'il survenait dans le cockpit d'un avion. La sûreté et la sécurité des systèmes informatiques sont donc des enjeux majeurs.

Avant de laisser la parole à M. Mallet, je veux remercier les différents intervenants. L'OPECST est le seul organisme interparlementaire : il joint donc la sagesse à l'innovation – je me garderai évidemment de dire à laquelle des deux assemblées il faut attribuer chacune de ces qualités. (Sourires.) Nous nous efforçons, en tout état de cause, d'être en amont des propositions législatives.

M. le ministre étant retenu par une réunion à l'OTAN, je vous remercie, monsieur Mallet, d'être venu, en son nom, conclure nos échanges. Je rappelle que

vous avez joué un rôle important dans l'élaboration du dernier Livre blanc comme du précédent.

Nous avons parcouru différents thèmes, en associant les approches civiles et militaires : c'est sans doute l'une des premières fois que la défense, l'OPECST et les organismes de recherche se réunissent autour d'une même table.

ALLOCUTION DE CLÔTURE DE LA MATINÉE PAR M. JEAN-CLAUDE MALLET, CONSEILLER SPÉCIAL DE M ; JEAN-YVES LE DRIAN, MINISTRE DE LA DÉFENSE

M. Jean-Claude Mallet, conseiller spécial de M. Jean-Yves Le Drian, ministre de la défense. Je vous remercie de votre invitation. Cette réunion illustre le rôle d'éclaireur vigilant qui est celui du Parlement sur des questions touchant à la défense, à l'économie et aux capacités de nos sociétés à résister à de nouvelles menaces, questions qui étaient déjà au cœur de la préparation du Livre blanc de 2008. Je m'efforcerai de vous exposer le point de vue du ministère de la défense sur ces nouveaux enjeux pour la sécurité nationale.

Les cyberattaques augmentent de façon exponentielle, qu'il s'agisse de bénins dénis de service, d'intrusions ayant pour but de piller des informations détenues par des acteurs privés de nos programmes d'armement, de paralysies d'infrastructures critiques ou de destructions de réseaux informatiques vitaux. Cette menace progresse à un rythme beaucoup plus rapide que celui des réponses qui lui sont apportées par nos entreprises et par les grands acteurs de la défense. Elle n'en est, soyons-en conscients, qu'à ses débuts, et nous commençons seulement à définir des stratégies de défense et d'attaque – puisque le Livre blanc de 2008 mentionne la lutte informatique offensive comme un nouvel instrument de défense, notamment dans le cadre d'une réplique. L'échelle de la menace, sorte d'archétype du conflit sans frontières, dépasse les normes habituelles de la guerre : il ne s'agit plus d'une confrontation directe entre États, y compris au regard de la dissuasion. Entre la destruction d'installations vitales, la prise de contrôle d'infrastructures critiques, à un niveau partiel ou global, la destruction du fonctionnement d'entreprises – illustrée par l'affaire Saudi Aramco –, le pillage d'informations ou la paralysie d'infrastructures et le soutien à des actions militaires – lequel figure désormais dans la doctrine militaire de certains pays –, les capacités sont insoupçonnées, et elles seront bientôt développées par des États.

Nous savons aussi qu'elles le seront, compte tenu de leur nature, par des groupes non étatiques – le cas échéant avec l'appui de certains États –, dans le but de mener des guerres asymétriques contre des États ou des gouvernements. Le développement du numérique démultiplie les capacités en matière de croissance économique, de connaissance et même de capacité de défense ou de lutte contre la criminalité ; aussi la numérisation fera-t-elle l'objet d'investissements massifs, comme l'ont confirmé le Président de la République et le Gouvernement. Nous devons aussi nous préparer à utiliser ces moyens de façon offensive, ce qui, au demeurant, est déjà le cas. Si les grands acteurs économiques et les partenaires du ministère de la défense ne s'organisent pas, nous en paierons le prix fort. Leon Panetta a évoqué un possible Pearl Harbor pour les États-Unis, événement

synonyme, pour la mémoire collective américaine, d'attaque brutale et imprévisible ayant détruit une partie importante des moyens de défense. Cette vision me semble rigoureusement exacte. Soit dit en passant, je pressens le moment où le ministère de la défense devra imposer à ses partenaires privés des normes de sécurité, dont le non-respect leur interdira tout simplement de lui fournir des moyens. Le sujet dont nous parlons est donc au cœur, non seulement de l'élaboration de doctrines futures, mais aussi d'un effort majeur du ministère de la défense et, au-delà, de l'ensemble de l'appareil d'État. Les moyens de l'ANSSI doivent impérativement être renforcés afin de compléter le spectre de nos capacités de défense en ces domaines.

Depuis plusieurs années, le ministère de la défense a créé une chaîne de commandement opérationnel relative à la cyberdéfense offensive et défensive ; il a commencé à investir, tant en moyens humains que techniques, pour répondre aux besoins des pôles du ministère et des armées, et développer une base industrielle et technologique. Plus généralement, l'État définit des doctrines qui seront débattues dans les mois et les années à venir, qu'il s'agisse de la protection des systèmes d'informations de l'État et des opérateurs d'importance vitale – l'organisation opérationnelle étant assurée par le ministère de la défense et coordonnée, au niveau gouvernemental, par le Premier ministre –, ou de la réponse à des attaques globales via les moyens juridiques, policiers et diplomatiques requis, ou des moyens plus spécifiques au ministère de la défense, en particulier en cas de menace pour les intérêts nationaux. Dans ce cadre, le ministère de la défense réfléchit à des capacités informatiques offensives, dont les autorités publiques, au plus haut niveau de l'État, pourraient décider de l'emploi – en l'occurrence, un emploi proportionné, discret et le plus efficace possible, en appui des actions militaires. Il est donc essentiel, je le répète, que les fournisseurs d'équipements et les prestataires de services du ministère de la défense adoptent des normes de sécurité, sous le contrôle vigilant des autorités en charge de la cyberdéfense.

J'évoquerai pour finir la dimension sociale et citoyenne. Une réserve citoyenne a été créée pour sensibiliser l'opinion et faire la promotion d'un esprit de cyberdéfense. Nous réfléchissons aussi à la mise en place d'une réserve opérationnelle qui permettrait à la société française de résister à un incident ou une agression de grande ampleur, au-delà des moyens que j'évoquais précédemment.

J'espère ne pas avoir dressé un tableau trop sombre. Le développement des capacités de cyberdéfense comme de capacités offensives est une ambition qui ouvre un champ formidable pour nos jeunes ingénieurs et nos militaires : c'est le meilleur des technologies et des intelligences, dont notre pays ne manque pas – les acteurs de la défense le montrent tous les jours –, qu'il faudra mobiliser. Aussi les questions que vous avez abordées représentent-elles des enjeux essentiels pour le Président de la République et le ministre de la défense.

M. Bruno Sido, sénateur, président de l'OPECST. Merci pour cet exposé conclusif, qui est comme le point d'orgue de nos discussions de ce matin. Je remercie aussi les différents intervenants pour la richesse de nos échanges.

DEUXIÈME PARTIE :
PRÉMUNIR LA SOCIÉTÉ CONTRE LE RISQUE DE LA DÉPENDANCE NUMÉRIQUE

I. PREMIÈRE TABLE RONDE : LA SÛRETÉ NUMÉRIQUE DANS LA GESTION COURANTE

Présidence de M. Bruno Sido, sénateur, président de l'OPECST

M. Bruno Sido, sénteur, président de l'Opecst. Après avoir parlé ce matin de sécurité numérique et de résistance des systèmes aux attaques, nous abordons cet après-midi un sujet tout aussi important, celui de la sûreté intrinsèque de ces systèmes. Nous examinerons successivement les questions de l'étendue de l'exposition aux risques de défaillance, de la fiabilité des appareils servant au diagnostic en matière de santé et de la capacité à certifier la validité des systèmes numériques.

Comme un certain nombre d'entre nous, j'ai grandi dans une société sans ordinateur. Notre premier contact avec l'informatique se faisait par l'initiation à des langages aux intitulés étranges, comme le cobol ou le fortran, qui permettaient de faire fonctionner un ordinateur dont les calculs se traduisaient par un amoncellement de cartes perforées.

C'est une banalité de pointer l'ampleur des progrès accomplis depuis, mais j'ai la conviction que la numérisation de la société en est au stade où, comme le nénuphar, elle ne remplit que la dixième partie du bassin, avant d'en occuper la moitié demain et la totalité après-demain.

L'aviation civile est un bon exemple de cette progression car elle emploie des logiciels dits critiques, c'est-à-dire qui ne doivent pas connaître de défaillance. Le Concorde a été, en 1969, le premier appareil à être équipé de commandes de vol électronique. Aujourd'hui, les commandes de vol d'un A380 comptent plus d'un million de lignes de codes. Demain, d'ici 2025, la navigation aérienne sera assurée par un système entièrement numérisé dont les codes compteront des millions de lignes. Au stade ultime de cette évolution, les avions de ligne seront devenus des objets numériques pouvant rectifier en permanence leur trajectoire en fonction de leurs perspectives d'atterrissage, de la météo et du trafic aérien. Cet exemple nous permet de mesurer l'ampleur du défi qui nous attend.

Produire des logiciels est une chose, vérifier leur validité en est une autre. Le logiciel de conception des trains d'atterrissage de l'A380 est six fois moins volumineux que ses logiciels de vérification. Les écoles françaises de mathématiques ont développé, à compter du milieu des années soixante-dix, des instruments comme l'analyse statique et la vérification formelle qui s'assurent de la validité de systèmes de plus en plus massifs à moindre coût. En dépit de l'excellence de nos chercheurs dans ce domaine et de l'intérêt de nos industriels pour ces questions, je ne suis pas sûr que les pouvoirs publics français aient conscience de l'importance de ce qui se profile. C'est pourquoi je souhaite que l'Office, dont c'est la vocation, soit saisi de ces questions.

La première table ronde de cet après-midi va nous conduire à nous pencher d'abord sur l'importance prise par les systèmes numériques dans les dispositifs de gestion courante. Cette dépendance fragilise *de facto* toute l'architecture sociale. La crainte cataclysmique du fameux bug de l'an 2000 est une anticipation, certes exagérée, de ce phénomène. La question est de savoir à quelle vitesse la réalité va finir par rattraper ce type d'appréhension. C'est une interrogation que je soumets à M. Gérard Berry.

M. Gérard Berry, professeur au Collège de France, membre de l'Académie des sciences et de l'Académie des technologies. Je suis ravi que vous ayez pris l'exemple de la navigation aérienne, domaine dans laquelle la France était très en avance. Il était devenu impossible de piloter des avions de chasse à la main. En outre, l'informatique a permis une navigation plus économique, plus légère et surtout plus sûre.

Elle est désormais partout et ses applications sont innombrables. Je vais vous parler aujourd'hui de ses dangers, mais ceux-ci ne doivent pas faire oublier ses succès, qui sont plus importants.

Il y a deux grands dangers liés à l'informatique : les bugs et l'inculture informatique.

Il faut savoir qu'un programme informatique est un système qui exécute exactement et obstinément des ordres extraordinairement détaillés, y compris ceux qu'on n'aurait pas dû lui donner, d'où les bugs. Cela ne signifie pas que tous les systèmes engendrent des bugs. En avionique, l'extrême sophistication des méthodes de développement et de certification des équipements informatiques permet de les éviter. En réalité, les bugs sont dus au manque de soin dans la fabrication des applications. C'est le cas pour les téléphones portables, les industriels ayant d'abord le souci de sortir de nouveaux produits le plus rapidement possible pour conquérir des parts de marché. Il est vrai que la qualité des téléphones portables n'est pas un enjeu vital, à la différence de celle d'un avion. Les équipements informatiques posent également beaucoup plus de problèmes dans les voitures que dans les avions, parce que la règle de base des constructeurs automobiles est de réduire les coûts.

Le manque de culture informatique est peut-être plus grave, dans la mesure où il est plus difficile d'y remédier qu'à un simple problème technique. Pendant très longtemps, nos dirigeants ont relégué l'informatique à une place ancillaire. Cela s'explique par le fait qu'ils sont généralement dépourvus de toute formation dans ce domaine, voire du simple bon sens qui leur permettrait de comprendre à peu près comment cela fonctionne. Faute de cette qualité, on a tendance à projeter sur ce sujet les compétences apprises ailleurs. Je me suis ainsi rendu compte que les ingénieurs avec lesquels j'ai été amené à travailler sur le projet de navette Hermès appliquaient à l'informatique des raisonnements de mécanique.

Pour contrer les bugs, les informaticiens, tant les chercheurs que les industriels, développent des techniques de génie logiciel ou de mathématique formelle, domaine où la France excelle. Malheureusement les techniques de génie logiciel ne bénéficient pas de la même considération que les techniques de génie mécanique.

Il faut donc promouvoir les systèmes qui marchent, car ils existent : on n'est pas obligé d'utiliser des programmes qui ne fonctionnent pas ! Si la commande publique en matériel informatique n'était pas obnubilée par le critère du moindre coût, l'État risquerait moins de bugs, dont le coût peut se révéler important : récemment, un bug affectant la fabrication d'un des transistors du dernier Pentium a coûté un milliard de dollars à Intel.

L'autre remède, c'est l'éducation. Aujourd'hui que tout est numérique, il est grand temps que les ingénieurs et les dirigeants soient éduqués à l'informatique. L'éducation à l'informatique fait d'ailleurs l'objet de travaux de l'Académie des sciences. Il faut absolument que les parlementaires se saisissent de ce sujet crucial : nous ne serons pas en mesure de fabriquer des systèmes fiables et exportables tant que la culture informatique ne sera pas généralisée dans notre pays. Comme le disait Jean Vilar, « si vous trouvez que l'éducation coûte cher, essayez l'ignorance. »

M. le président Bruno Sido. Monsieur Marko Erman, comment percevez-vous les progrès de la numérisation globale de la société ? Ne risquent-ils pas de générer à terme un grave risque de système ?

M. Marko Erman, senior vice president, recherche et technologie, chez Thales et membre de l'Académie des technologies. Je voudrais vous sensibiliser à l'importance des données dans la société numérique. Notre société de l'information se caractérise par une production massive de données numériques de toutes sortes et la capacité de les interconnecter et de faire communiquer les personnes, les objets et les différentes organisations. Ces données sont en quelque sorte la matière première de la société de l'information. Elles représentent un enjeu économique, stratégique, voire culturel, majeur. C'est sur cet enjeu et ses risques associés que je voudrais centrer mon intervention.

Ces données viennent de partout et de tout le monde. Chacun de nous crée des données, soit de façon passive, à travers son identité numérique ou la dématérialisation d'actes administratifs, soit de façon active, par exemple en participant à des réseaux sociaux. Les entreprises, les banques, les institutions à travers leurs activités de production, de gestion, d'interaction avec les clients, en produisent beaucoup. De plus en plus de données sont également produites par des systèmes dits embarqués, qui, à travers différents capteurs, interagissent et recueillent des informations liées à leur environnement. En 2012, 2,5 Exabyte de données ont été produites chaque jour, soit dix fois plus qu'il y a à peine cinq ans, et 50 000 fois plus que la somme de toute la littérature de l'humanité. Ces chiffres donnent le vertige, et on pourrait les multiplier à loisir. Nous sommes entrés *de facto* dans l'ère des *big data*, c'est-à-dire des ensembles de données dont la taille va au-delà de la capacité actuelle des logiciels de gestion.

La problématique des données est indissociable de celle des réseaux de communication qui permettent de les échanger, de les stocker et de les consulter.

D'ores et déjà, toutes nos infrastructures – aéroports, gares, stations de métro, lignes ferroviaires, autoroutes, centrales d'énergie, etc. –, leurs systèmes de contrôle et les outils industriels sont interconnectés, voire connectés à Internet, directement ou indirectement, de manière permanente ou temporaire. Basés sur ces technologies de l'information – capteurs, données, communication –, des systèmes extrêmement complexes deviennent possibles, tels que les villes intelligentes, les *smart cities* ou les réseaux de distribution d'énergie du type *smart grids*.

Les systèmes qui pilotent nos infrastructures produisent beaucoup de données mais, dans la majorité des cas, ne les exploitent pas. Ils réagissent en fonction de celles « du moment » – alertes remontées par des capteurs, contrôle de la validité d'un titre de transport, par exemple – mais ne tirent partie ni du passé, ni de la totalité des données disponibles pour prendre ou proposer une meilleure décision. Ce n'est pas étonnant : jusqu'à récemment, le trop grand volume de celles-ci et les ressources de calcul nécessaires pour les traiter rendaient cette tâche difficile.

Aujourd'hui, les progrès dans le domaine de l'algorithmique – le réseau Internet, le *cloud* – et les capacités accrues de traitement des données sont autant d'atouts supplémentaires pour s'attaquer à ce défi. Des approches mathématiques adaptées doivent permettre d'extraire des informations pertinentes. Il est important de comprendre que ceci peut se faire hors hypothèses *a priori* : on découvre en quelque sorte l'information cachée. C'est bien cela qui donne au couple « données brutes – information extraite » une valeur économique et stratégique forte.

La valeur économique fonde le « *business model* » des grandes entreprises du web, telles Google, Facebook ou Twitter. L'objectif de ces sociétés est de collecter le maximum d'informations sur le plus grand nombre d'usagers possible

pour leur offrir un service personnalisé. Des acquisitions récentes ont montré que la valeur de celles-ci est directement liée à la taille de leur base clients.

Lorsque le champ des données inclut des éléments relatifs aux activités industrielles, financières, au transport, à l'énergie, son caractère stratégique devient évident. Les grands pays, et d'abord les États-Unis, l'ont parfaitement compris. Ils en exploitent formidablement le potentiel économique. Mais des initiatives, comme le *Patriot Act*, montrent, s'il en était besoin, que la valeur stratégique des données est au centre des préoccupations liées à la sécurité nationale. Aujourd'hui, et plus encore demain, les grands pays qui connaissent un développement économique rapide, comme l'Inde, la Chine ou le Brésil, emprunteront le même chemin. Il est certain que ces pays voudront exploiter eux-mêmes cette matière première.

La France ne peut rester indifférente à ce qui est un enjeu majeur pour notre pays aussi, et, au-delà, pour l'Europe.

Pour relever ce défi, elle ne manque pas d'atouts, dont en premier lieu l'excellence de notre recherche en mathématiques – je rappelle que cette science est à l'origine des algorithmes nécessaires aussi bien à l'exploitation des données qu'à leur protection. C'est pourquoi elle doit être préservée et renforcée.

Le comité interministériel pour la modernisation de l'action publique du 18 décembre 2012 a présenté la transition numérique comme « un formidable levier de modernisation de l'action publique », porteur de valeurs « d'égalité, de neutralité, de transparence, d'efficacité et d'adaptation ». Cette transition comportera quatre volets : l'amélioration du service à l'usager ; le développement des services numériques ; l'ouverture de l'administration et des données publiques ; la modernisation des systèmes d'information.

La démarche « *Open Data* » et la création de la structure ETALAB s'inscrivent parfaitement dans ce souci d'ouverture des données publiques, permettant de créer de nouveaux services. C'est pourquoi il faut la soutenir. Cependant, si on veut se prémunir contre les risques potentiels, il est important de prendre en compte dès maintenant la problématique de la sécurité, en même temps que celle des formats et du stockage.

Ce qui est vrai pour les données publiques l'est encore plus pour toutes les autres.

Du coup, la question de la fiabilité et de la protection des informations devient cruciale. Elle nous ramène directement à la problématique sur les données dont elles sont extraites. Au-delà des problèmes de cybersécurité, absolument essentiels, il faut établir les conditions qui permettront d'assurer l'intégrité des données et la confiance numérique. Cela nécessite de maîtriser les technologies de

stockage de celles-ci, les réseaux de transmission et bien évidemment l'analyse et l'exploitation.

On le sait, l'informatique en nuage offre des solutions économiques et performantes pour le stockage et est capable de fournir des services à la demande. Au travers de la création de sociétés comme CloudWatt et d'autres, la France commence à se doter de solutions de *cloud* sécurisées. C'est absolument nécessaire dans ce contexte.

Le réseau Internet, qu'il soit fixe ou mobile, assure l'indispensable interconnexion entre tous ses points – serveurs, capteurs, usagers, etc. Il est considéré comme intrinsèquement résistant aux chocs puisqu'il s'agit d'une immense toile qui peut supporter la perte d'un ou plusieurs nœuds de connexion. Cependant, si, dans sa description logique, il se compose de plusieurs centaines d'opérateurs, offrant ainsi de la redondance, le réseau physique a, quant à lui, une réalité moins diversifiée. Certaines catastrophes naturelles récentes ont montré la fragilité des réseaux de communication. Il est donc également essentiel d'améliorer leur résilience. Pour ce faire, il est nécessaire que l'analyse des risques prenne en compte les cas exceptionnels, voire aberrants.

J'ai essayé de vous faire partager ma conviction que les données vont jouer un rôle essentiel dans la société et l'économie numérique. Leur valeur économique et stratégique est d'ores et déjà établie, mais les possibilités dépassent l'imagination. Il est indispensable de maîtriser cette évolution en étant lucide sur les risques potentiels. Mme la ministre déléguée Fleur Pellerin a récemment déclaré : « Si la sécurité des systèmes d'information n'est pas assurée, aucune économie moderne ne peut prospérer ». Cela nécessite de garantir la sécurité des données, de mettre en place des opérateurs de confiance et de promouvoir une approche de régulation, de préférence à une approche purement réglementaire.

M. le président Bruno Sido. Le secteur de la santé bénéficie, comme tous les autres secteurs, des progrès de la numérisation. L'audition du président de l'Académie des technologies nous a fait découvrir les perspectives intéressantes de la « domomédecine » pour les soins à domicile. Cependant, une défaillance des systèmes constituerait une menace directe pour la santé des personnes. Comment peut-on garantir, monsieur de la Boulaye, la sécurité des systèmes numériques œuvrant dans ce secteur sensible ?

M. Olivier de la Boulaye, directeur du développement du secteur santé d'Altran. Je vous répondrai à travers une illustration : le projet PICADo, premier système opérationnel de domomédecine. Cela me permettra de vous présenter les solutions que nous pouvons, nous, les industriels, proposer pour sécuriser l'utilisation des données de santé.

Je rappelle que la domomédecine est un terme inventé par François Guinot, Président honoraire de l'Académie des Technologies, après la parution du

rapport de cette Académie « Le patient, les technologies et la médecine ambulatoire » et repris à l'occasion de la journée Télésanté organisée Conseil Régional de Champagne-Ardenne le 4 novembre 2009. La domomédecine se définit comme l'ensemble des actes et soins, parfois complexes, dispensés au domicile du patient ou durant ses activités socio-professionnelles, au moins comparables en quantité et qualité à ceux effectués à l'hôpital voire de meilleure qualité, s'appuyant sur des technologies modernes. Elle vise à privilégier le maintien à domicile ou en activité et à stimuler le progrès médical.

C'est le cas par exemple de la chrono chimiothérapie, une des thérapies du projet PICADo. Le patient enverra à son médecin, *via* des capteurs communicants, des éléments tels que sa température ou son niveau d'activité, afin que celui-ci puisse adapter son traitement et proposer en temps réel le meilleur moment d'administration et les meilleurs dosages.

Ce type de dispositif doit évidemment respecter le cadre législatif et réglementaire existant, c'est-à-dire le décret du 19 octobre 2010 relatif à la télémédecine et la loi « informatique et libertés ». Les industriels que nous sommes doivent en outre tenir compte des préconisations du conseil de l'ordre des médecins et de celui des pharmaciens.

Selon l'article 34 de la loi « informatique et libertés », « le responsable du traitement [d'une donnée de santé] est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. ». Le respect de cet article se décline selon cinq grands principes : la finalité des données ; leur pertinence – nous n'utilisons que celles dont nous avons réellement besoin – ; leur conservation pendant un temps limité – c'est le droit à l'oubli ; la sécurité et la confidentialité ; le respect des droits des personnes, qui nous impose, par exemple, de nous assurer que le patient accepte que ces données soient utilisées.

Le projet PICADo concerne quelques centaines de patients et associe à Altran des sociétés plus petites comme Axon, Voluntis, Bluelinea ou FSI, soit des partenaires aux parcours très différents, qui n'ont pas tous la même capacité à respecter les normes imposées par nos tutelles.

Un tel système de santé suppose trois niveaux de mise en place. Au niveau des processus, nous nous interrogeons sur la finalité ou l'usage. C'est la notion d'authentification, *via*, par exemple, la carte de professionnel de santé (CPS) ou la carte Vitale pour le patient. Nous cherchons ensuite comment collecter et utiliser ces informations, qui peuvent être utilisées à des fins, non seulement médicales, mais aussi médico-légales – d'où l'importance de mettre en place des systèmes garantissant une parfaite traçabilité. Deux nouveaux enjeux sont apparus récemment dans l'univers de l'e-santé : l'impact du sans-fil, qui, comme toute

innovation, appelle de nouvelles solutions en termes de sécurité, et la problématique de la consommation énergétique.

Après les processus, notre réflexion porte sur les données. Nous bénéficions en la matière d'un cadre normatif assez précis, notamment en ce qui concerne l'hébergement des données de santé, soumis à l'agrément de l'Agence des systèmes d'information partagés de santé (ASIP). Cela suppose le respect d'un cahier des charges très précis en matière de redondance, de sécurisation et de traçabilité des données notamment.

Il faut enfin considérer le niveau applicatif, qui concerne la conception des logiciels, l'ergonomie ou la gestion des habilitations : beaucoup de failles de sécurité sont dues à des problèmes d'habilitation. Quant à la conception des logiciels, elle doit respecter un certain nombre de référentiels internationaux pour les systèmes d'information de santé, tel l'*Integrating the Healthcare Enterprise*, l'IHE. Ils nous permettent de respecter au mieux les très nombreuses normes en vigueur, qui sont en outre extrêmement complexes. Les seules directives européennes imposent à un projet tel que PICADo le respect de la norme ISO 13485, qui précise les exigences des systèmes de management de la qualité pour les dispositifs médicaux, de la norme ISO 62304, qui définit les exigences du cycle de vie des logiciels de dispositifs médicaux, et de la norme ISO 60601, qui fixe les exigences de développement d'un dispositif médical – pour ne parler que des plus importantes.

Je ne peux pas terminer mon propos sans évoquer deux notions. D'abord celle du « *bring your own device* ». Aujourd'hui, un médecin va plutôt utiliser son iPhone ou son iPad que son poste de travail pour transmettre des données, ce qui induit de nouveaux problèmes de sécurité des systèmes d'information de santé. La bonne nouvelle, c'est que nous avons des solutions pour y remédier.

L'autre notion est celle de modèle économique, qui appelle la capacité à proposer une itération et une progression dans la mise en place du niveau cible de conformité aux normes. En tant qu'industriel, nous souhaitons pouvoir à la fois conseiller un fabricant de dispositifs médicaux, qui est souvent une petite entreprise, et un professionnel de santé quant au bon niveau de risque.

M. le président Bruno Sido. Le dernier thème de cette table ronde va nous permettre de mettre en valeur la qualité remarquable de la recherche française dans le domaine du numérique, puisque c'est dans le cadre de l'Institut national de recherche en informatique et en automatique (Inria) qu'ont été mis au point les premiers dispositifs de vérification de la validité intrinsèque des programmes. Pourriez-vous, monsieur Gilles Dowek, nous expliquer de manière pédagogique les tenants et les aboutissants de ce problème scientifique complexe ?

M. Gilles Dowek, directeur scientifique adjoint à l'Institut national de recherche en informatique et en automatique (Inria). Les systèmes informatiques sont partout, pour le mieux en général. Ils permettent par exemple d'améliorer la qualité des soins médicaux, *via* notamment l'imagerie médicale ou la robotique chirurgicale ; ils facilitent l'accès à la connaissance, appelé à connaître une transformation radicale avec la mise en place d'e-universités. Ils ont bouleversé les modes de communications interpersonnelles. On ne peut pas, bien entendu, passer sous silence l'accroissement considérable de la productivité qu'on leur doit. C'est précisément parce que l'informatique nous apporte tous ces bénéfices que leur dysfonctionnement peut provoquer des dommages, tant matériels qu'humains, à la mesure de cette omniprésence.

On appelle domaines critiques ceux dans lesquels le dysfonctionnement d'un système informatique provoque des conséquences graves. On en compte au moins quatre : les transports, la santé, l'énergie – on a évoqué la sûreté des centrales nucléaires –, la banque et plus largement les services.

Définir les menaces pesant sur un système informatique suppose de faire la distinction traditionnelle entre sûreté et sécurité : c'est la différence entre défaillance involontaire et action malveillante. Un crash aérien, par exemple, peut être consécutif à une panne de son moteur : c'est là un problème de sûreté. Mais s'il est dû au déclenchement d'une bombe placée dans l'avion, il s'agit d'une faille de la sécurité.

Fabriquer des objets qui fonctionnent n'est certes pas un objectif propre à l'informatique. Cependant, les objets informatiques présentent la spécificité d'être les plus complexes de toute l'histoire de l'industrie humaine. Un programme compte plusieurs dizaines de millions de lignes, contre quelques dizaines de milliers dans un roman. C'est encore plus vrai s'agissant des matériels : il y a plusieurs milliards de transistors dans un processeur, contre cinq ou dix dans un poste de radio. Il est humainement impossible de construire un système aussi complexe sans se tromper. De plus, l'interconnexion des systèmes produit des bugs généralisés ou en cascade.

Étant donné le caractère faillible des êtres humains, le développement de logiciels ne peut pas être une activité exclusivement humaine. C'est la raison pour laquelle on utilise des outils informatiques pour concevoir des systèmes sans bugs. Ces outils s'appellent l'analyse statique, la vérification dans un modèle, la preuve, *etc*. Ils sont le fruit de recherches fondamentales en théorie de la démonstration, en théorie des langages de programmation et en combinatoire, ainsi que dans d'autres domaines à la frontière de l'informatique et des mathématiques. Ils ne sont pas plus interchangeables que ne le sont un marteau, un tournevis et une clé à molette : ils traitent des problèmes différents et doivent souvent être combinés. Ensemble, ils constituent une boite à outils qu'on appelle les méthodes formelles.

Ainsi, les algorithmes et les programmes de contrôle aérien peuvent être très complexes, mais la tâche qu'ils doivent réaliser est très simple : maintenir une distance de séparation minimale entre les avions à tout instant.

Lorsqu'on a cette spécification et ce programme, il est possible, en utilisant des outils appropriés, de démontrer, au sens mathématique du terme, que tel programme vérifie telle spécification.

La preuve de programme a été appliquée à de nombreux cas, notamment aux trains de la ligne 14 du métro parisien ou à certains compilateurs utilisés par Airbus.

En conclusion, la France fait partie des pays leaders en matière de recherche dans les méthodes formelles. Il y a, dans notre pays, un véritable potentiel de développement pour une industrie dans ce domaine.

Une manière de soutenir ce développement et d'améliorer la sûreté et la sécurité des logiciels que nous utilisons tous les jours est d'imposer, lors de la commande publique de systèmes critiques, l'utilisation de méthodes formelles, par exemple en utilisant le vocabulaire des critères communs, qui mesure la qualité d'un projet sur une échelle allant de EAL-1 à EAL-7. C'est déjà le cas, mais ce pourrait être systématique.

M. le président Bruno Sido. M. Bolignano va maintenant nous expliquer comment on peut tenter de développer, au niveau commercial, une activité de vérification de la sûreté intrinsèque des logiciels.

M. Dominique Bolignano, président directeur général de Prove&Run. Je vais vous parler de l'état actuel de l'utilisation des méthodes formelles dans l'industrie et du potentiel de celles-ci.

Pour ce faire, je répartirai les trois catégories de méthodes formelles dont a parlé Gilles Dowek en deux groupes.

Celles du premier groupe – analyse statique et vérification dans un modèle – sont les plus simples d'utilisation. Elles permettent de répondre à des questions précises, mais plus limitées, et d'éviter certains types d'erreurs informatiques ou sur certaines catégories de logiciels. Gérard Berry a donné plusieurs exemples de leur application dans les transports, notamment dans l'aéronautique. Ce sont, de loin, les plus utilisées dans l'industrie.

Une dizaine de sociétés – françaises ou contrôlées par de grands groupes français – commercialisent ces technologies. Malgré un grand potentiel de croissance, ces sociétés restent de taille modeste – entre 10 et 200 personnes. Elles n'en ont pas moins une grande importance pour la sûreté et la sécurité numériques.

Le deuxième groupe de méthodes formelles concerne la preuve de programme : il faut l'appliquer là où les techniques du premier groupe ne réussissent pas, car elle est beaucoup plus coûteuse et demande plus de temps. En revanche, son domaine d'application est beaucoup plus vaste. Elle couvre à peu près tous les secteurs qu'on a cités et permet de répondre à un nombre de questions beaucoup plus important.

Il en est ainsi pour la téléphonie mobile. La plupart des informations importantes, autant pour les entreprises que pour les particuliers, passent par les téléphones, et celles qui n'y passent pas sont accessibles à distance grâce à eux. C'est donc un point de vulnérabilité très important.

Actuellement, à chaque nouvelle version, quelques semaines suffisent pour que les téléphones de dernière génération – comme ceux d'Apple ou d'Android – soient crackés, c'est-à-dire attaqués et cassés dans leur sécurité. Les pirates ou les attaquants exploitent des vulnérabilités, qui sont des erreurs logicielles. Ce sont les bogues – ou bugs dont parlait Gérard Berry. Les bogues en matière de sûreté ont moins de répercussions, mais en matière de sécurité, quelques-uns suffisent pour mener une attaque de grande envergure. Voilà pourquoi on essaie de s'approcher le plus possible du « zéro faute ».

Ces erreurs sont exploitées pour des besoins relativement modestes, mais elles pourraient l'être pour lancer des attaques beaucoup plus graves. Cela nous renvoie aux propos qu'a tenus ce matin le représentant du ministère de la défense.

Je citerai deux exemples liés à la téléphonie mobile.

Le premier concerne les entreprises. La plupart des cadres utilisent leur téléphone à des fins aussi bien professionnelles que personnelles : ils consultent des mails et peuvent charger des applications à la fiabilité douteuse. Or les erreurs logicielles peuvent être utilisées pour corrompre et faire du cyberespionnage à relativement grande échelle, ce qui peut avoir des répercussions dramatiques sur l'entreprise.

Ces erreurs pourraient être évitées par une bonne application des méthodes formelles, en particulier de la preuve de programme. Certes, cela coûte cher et est difficile à faire, mais c'est faisable.

Deuxième axe : le paiement par téléphone. S'il y a eu beaucoup d'avancées grâce à la carte à puce, le téléphone reste un élément vulnérable dans la mesure où l'on a remplacé des terminaux de paiement relativement sécurisés par des objets qui le sont beaucoup moins.

Quant à la banque à domicile, qui n'est pas considérée comme un moyen de paiement mais permet de faire des virements, elle est encore plus vulnérable.

Il ne s'agit pas d'appliquer ces techniques sur tout le logiciel. En effet, les téléphones peuvent comporter jusqu'à plusieurs dizaines de millions de lignes de codes. Les architectures modernes permettent de se focaliser sur une « base de confiance », qui ne fait que quelques dizaines de milliers de lignes de codes : en s'attaquant à celles-ci, on peut vraiment s'approcher du « zéro défaut » s'agissant des parties critiques et éviter ces erreurs.

On a dit ce matin que cette problématique connaissait une croissance exponentielle. Je le confirme : nous n'en sommes qu'au début.

L'utilisation des méthodes formelles reste très modeste, essentiellement pour des problèmes liés à leur mise en œuvre et au manque de disponibilité d'experts dans ces domaines. Cela étant, la nouvelle société que j'ai créée a pour objet de les appliquer à grande échelle : des raisons objectives m'amènent à penser que c'est possible.

Nous nous trouvons aujourd'hui dans une situation très proche de celle d'il y a trente ans, au moment de la conception en 3D. Des sociétés comme Dassault Systèmes, qui est devenu le numéro un mondial dans son domaine, ont transformé la manière dont le développement était fait. Aujourd'hui, l'enjeu est encore plus grand, car le potentiel est probablement beaucoup plus important.

Pour terminer, je rejoindrai Gilles Dowek en disant que c'est le moment de se lancer. Je le montre moi-même en investissant beaucoup. Les pouvoirs publics pourraient de leur côté favoriser l'utilisation de ces méthodes formelles, afin d'enclencher un cercle vertueux.

M. le président Bruno Sido. Je vous remercie. Le débat est ouvert.

Débat

M. Michel Cosnard, président directeur général de l'Inria. Ma question s'adresse à Dominique Bolignano : quel serait le bon modèle économique, susceptible de favoriser l'usage de méthodes de développement garantissant une meilleure qualité et une meilleure fiabilité des logiciels critiques ?

M. Dominique Bolignano. C'est un modèle que j'ai déjà testé dans de précédentes entreprises et que je compte appliquer à plus grande échelle. Il consiste à développer des composants réutilisables clés avec les méthodes formelles et à les licencier pour que, dans un deuxième temps, les clients utilisateurs demandent à se les approprier, licencient les outils et adoptent la technologie. Il faut entrer dans un cercle vertueux en démontrant que c'est faisable et utile, afin que les entreprises soient prêtes à investir.

M. Michel Cosnard. Y a-t-il un secteur d'activité privilégié ?

M. Dominique Bolignano. Oui. Nous allons commencer par le domaine de la téléphonie mobile, où il y a énormément à faire. Mais il y a aussi beaucoup à faire dans l'aéronautique, l'automobile et probablement aussi dans le domaine médical.

M. le président Bruno Sido. Monsieur le professeur, on nous a dit qu'il était humainement impossible, dans un programme de plusieurs milliers de lignes de code, de ne pas introduire quelque part une erreur, un bug. Mais ce bug, introduit involontairement par l'homme, se déclenchera-t-il de façon aléatoire ou systématique ?

M. Gérard Berry. Il est très difficile de vous répondre. Sur du *hardware*, sur un circuit, il y a des probabilités de panne qui sont chiffrées, raisonnables et mesurées. Sur un logiciel, la question n'a pas vraiment de sens. En effet, on peut ne jamais voir le bug qui existe. En général, il ne se produira pas, sauf si des hackers la cherchent. Car avec des bons hackers, la probabilité devient 1.

Ainsi, une faculté américaine a montré qu'on pouvait prendre le pouvoir sur 50 % des pacemakers livrés aux États-Unis : on peut les arrêter, envoyer 800 volts, faire absolument ce que l'on veut. Ce bug ne se produira jamais sur un humain normal, mais on peut le fabriquer exprès.

Il n'est donc pas ridicule de viser le « zéro défaut ». Cela demande de modifier le design. Il n'y a pas que la vérification, mais aussi la façon de concevoir les applications. Nous avons ainsi fabriqué des langages, dont la définition est mathématique et dont le mode d'emploi mélange formules mathématiques et commentaires en anglais.

Pour les bugs modernes, le danger réside donc essentiellement dans les hackers.

Mme Sylviane Toporkoff de l'Inria. Il existe maintenant des sociétés de hackers, qui sont très compétents. Fait-on systématiquement appel à elles lorsqu'on réalise un programme ?

M. Gérard Berry. Oui, cela arrive. D'assez nombreux hackers se sont fait embaucher, notamment par AT&T dans les télécoms.

Dans les sciences aussi, on fait de même. Après le bug d'Ariane, un grand informaticien, qui n'est pas du tout un hacker, a ainsi été employé pour analyser des programmes parce qu'il a une aptitude à découvrir des bugs là où les autres n'en trouvent pas.

Le problème est que ce n'est pas en se faisant embaucher par l'État français que les hackers gagnent le plus d'argent. Et donc, on n'a pas forcément les meilleurs …

M. Olivier de la Boulaye. Aujourd'hui, c'est le client qui définit le prix. Nous aimerions avoir recours à l'ensemble des méthodologies qui pourraient améliorer la sûreté des logiciels. Mais les clients ne sont pas forcément disposés à faire appel à une société comme celle de M. Bolignano.

Il faudrait proposer une démarche itérative. L'important est de se donner une certaine durée pour avoir un cap et anticiper ce cap. Les méthodes qui sont proposées le permettent.

Nous nous intéressons aussi beaucoup à la « base de confiance », qui permet de travailler sur un socle que l'on peut ensuite étendre progressivement, et d'apporter une première réponse aux contraintes économiques que l'on rencontre dans ce genre de projets.

M. Jean-Yves Le Déaut. On nous a indiqué ce matin que l'informatique était une suite de couches successives de travaux qui continuaient à être utilisés et qu'il était impossible d'aller explorer la totalité des réalisations anciennes.

On nous a dit aussi qu'aujourd'hui, elle était faite de systèmes intégrés, de briques associées les unes aux autres. Êtes-vous capables de vérifier qu'il n'y a pas de problème entre les briques et d'empêcher des personnes malveillantes de s'introduire dans le système d'intégration ?

M. Dominique Bolignano. Il est en effet possible de passer entre les couches et d'aller en dessous des logiciels. Ces deux problèmes peuvent être évités en choisissant les bonnes architectures. Il ne suffit donc pas d'appliquer les méthodes formelles.

En matière de téléphonie mobile, nous avons ainsi réussi à convaincre les principaux fabricants de téléphones de modifier leur architecture, précisément pour aller mettre, sous les couches de logiciels, les parties que l'on pouvait véritablement sécuriser.

M. Gérard Berry. Attention : toute l'informatique n'est pas vieille ! Elle est même principalement récente. Il s'écrit beaucoup plus de programmes maintenant qu'il ne s'en est jamais écrit. Mais les problèmes liés à la vie des appareils se posent effectivement parce qu'à l'époque, on ne se préoccupait pas de cela.

Il faut absolument fabriquer des composants de très haute qualité. D'où l'importance des procédures et des contraintes de certification. En avionique, il y a ainsi des procédures de certification internationales obligatoires et des réciprocités entre les pays. En revanche, dans le nucléaire, il n'y a que des procédures de certification nationales, nettement plus indicatives et variables selon les pays. Au

Japon, par exemple, certaines normes valables dans les années cinquante sont restées les mêmes.

La qualité des règles imposées par les États est absolument essentielle. Or en matière de santé, notamment, les normes ne sont pas tout à fait définies.

M. Olivier de la Boulaye. On voit bien à cet égard que les niveaux d'exigence ne sont pas les mêmes pour un dépistage et la prise en charge d'un acte médical.

M. Gilles Dowek. Il est beaucoup plus facile de développer des produits de qualité en utilisant des méthodes formelles au moment où on les développe, que de revenir sur des vieux codes d'il y a dix ou vingt ans, ou même de vieux algorithmes. En contrôle aérien, on m'avait demandé de démontrer la correction d'un algorithme ; je n'ai pas réussi et j'ai proposé mon propre algorithme. C'est de cette manière que l'on peut faire avancer les choses : davantage par une « co-conception » – conception de l'objet et de sa preuve en même temps – que par un retour sur le passé.

Ensuite, il ne suffit pas que les composants qui sont assemblés soient sûrs pour que l'ensemble le soit aussi. Mais les méthodes formelles peuvent s'appliquer aussi bien pour démontrer la sûreté de composants que celle de l'assemblage. Si cette dernière constitue un problème plus difficile, l'objectif est bien la sûreté globale, qui n'est jamais que celle du maillon le plus faible.

M. Michel Cosnard. Gilles Dowek a évoqué les critères EAL de 1 à 7. J'aimerais qu'il les précise et nous donne quelques exemples et, éventuellement, des recommandations sur leur utilisation. Y a-t-il des cas où un niveau minimum d'exigence serait souhaitable ? Si oui, comment le traduire en obligation réglementaire ?

M. Gilles Dowek. Je reviens sur une autre question que vous avez posée tout à l'heure, relative à la probabilité qu'un bug se produise.

Prenons l'exemple du bug du Pentium, évoqué par Gérard Berry. Nous sommes face à un circuit qui fait des multiplications. Si on essaie de multiplier 3 par 4, cela fait 12 ; en revanche, si on multiplie 0 par 0 – et c'est là qu'il y a un bug – cela fait 256. S'interroger sur la probabilité que ce bug se produise revient à s'interroger sur celle que l'utilisateur de la calculette décide de faire cette multiplication de 0 par 0.

Cela nous amène à la première méthode, que personne n'a mentionnée, consistant, pour vérifier que des programmes sont corrects, à les tester, et donc à les utiliser. On fait une, puis trois, puis dix multiplications. Si le résultat est exact pour dix opérations, on se dit que le programme ou le circuit semble correct, et l'on s'arrête là. Cela définit les niveaux EAL les plus bas, soit 1 ou 2.

Il y a ensuite, au milieu de la gamme, d'autres critères. On demande au développeur d'exprimer formellement, sans établir de preuve, mais de manière très précise et mathématique, la spécification du programme.

Ce n'est qu'aux niveaux 6 et 7, les plus élevés, que l'on demande au développeur, non seulement d'exprimer ainsi ce que doit faire le programme, mais aussi de démontrer qu'il fait bien ce que l'on attend de lui.

Ces critères correspondent à des niveaux d'exigence et de coût variables. Pour certaines applications, le bug n'est pas très grave : c'est le cas par exemple pour un DVD, au contraire d'un avion de ligne. Mais parfois il se mesure en milliards de dollars. Or pour anticiper un bug d'un milliard de dollars, on peut s'offrir beaucoup de méthodes formelles …

M. Jean-Yves Marion, responsable du Laboratoire de haute sécurité en informatique de Nancy. La sûreté informatique, le fait que les programmes n'aient pas de bugs, est importante. Mais la sécurité ne se réduit pas à cela. On peut attaquer un programme quasiment sans bug en utilisant l'ingénierie sociale, c'est-à-dire en contournant les problèmes d'usage au niveau des utilisateurs. D'où l'intérêt des systèmes de protection tels que les pare-feu, les antivirus ou les systèmes de virtualisation.

M. Marko Erman. Je suis d'accord avec vous. La sécurité n'est pas une caractéristique purement technique. Elle se conçoit au niveau d'un système.

Nous faisons des audits de cybersécurité, soit en anticipation à la demande des entreprises, soit en *post attack*. Comme dans les accidents d'avion, le facteur humain est souvent celui qui fait casser le système. Dans un système informatique totalement fermé, un immeuble blindé, si les personnels introduisent des clés USB non contrôlées, cela peut être catastrophique.

Au-delà de la sécurité technique, il faut s'intéresser à la sécurité physique, aux protocoles, aux process, à l'organisation et à la formation – *via* une sorte de labellisation ou de certification des personnes. De fait, lorsque la technologie est tellement diffusée, que toute personne est dans le système, la situation devient très difficile.

On progressera dans la sécurité quand le plus grand nombre des citoyens sera conscient des risques. Il ne s'agit pas de devenir paranoïaque, mais c'est en connaissant les risques que l'on peut se comporter correctement et s'en protéger.

M. Jean-Yves Le Déaut. Lorsque je demande à mes étudiants de Sciences Po de situer le bug informatique sur une échelle des risques, ils le classent en dernier ! Je pense que le citoyen n'a pas pris conscience de l'existence du risque informatique.

Les bienfaits de l'informatique sont avérés, mais nous devons nous prémunir contre les risques qu'elle entraîne et les attaques. L'objectif de cette table ronde est aussi de savoir s'il faut faire évoluer la législation ou mettre en place une régulation dans ce domaine.

M. Gilles Dowek. C'est précisément parce que les bienfaits de l'informatique sont nombreux que les risques existent.

M. Gérard Berry. À l'heure actuelle, les gens peuvent passer de l'absence totale d'inquiétude à l'angoisse. Ces deux attitudes absurdes prouvent qu'ils ignorent totalement ce qu'est l'informatique. Or la seule façon de maîtriser un risque, ou un bienfait, c'est d'en comprendre la nature. Il est sûr qu'un travail de fond s'impose dans ce domaine. L'éducation a un rôle essentiel à jouer à cet égard.

M. le président Bruno Sido. Vous avez parfaitement raison. Cela étant, les gens supportent de moins en moins les contrariétés – que les trains arrivent ou partent en retard, ou que les téléphones ne fonctionnent plus. Après tout, la panne d'Orange n'était pas particulièrement gênante, même si on n'a pas pu téléphoner pendant plusieurs heures.

M. Jean-Yves Le Déaut. Monsieur Berry, je vous rejoins sur le fait que les gens passent de la négation du risque à sa surestimation et sur l'ignorance en informatique. Si les sujets que l'Office étudie en amont de la législation sont ceux qui font débat dans la société – OGM, ondes électromagnétiques, réchauffement climatique, vaccins, nucléaire… –, il arrive que certains ne donnent pas lieu à débat. C'est ce qui est arrivé avec les OGM : en 1991, la transposition d'une directive européenne était passée dans l'indifférence générale. Il a fallu attendre cinq ans, soit les exportations de soja américain, pour que les OGM deviennent un problème politique. Avec les nanotechnologies, nous avons connu à peu près le même phénomène.

Si l'on aborde un sujet très tôt, cela n'intéresse absolument personne, et si on le fait trop tard, on nous prête l'intention de vouloir justifier certaines positions. Ces sujets sont très compliqués : il est difficile de se prononcer en amont des évolutions techniques et de comprendre l'incidence qu'elles auront sur la société.

M. Claude Kirchner. Je voudrais revenir sur la panne de France Télécom. Certes, il était très inconfortable de ne pas pouvoir téléphoner pendant onze heures. Mais cette panne a eu des conséquences plus larges qu'on n'avait pas envisagées : des sociétés importantes, qui faisaient passer leur cellule de gestion de crise par la téléphonie mobile, ont arrêté complètement leur activité lorsqu'elles se sont rendu compte qu'elles n'étaient plus capables de gérer une éventuelle crise.

Il ne faut pas oublier le rôle essentiel que joue la maintenance. Un logiciel a une vie et peut connaître, au cours de cette vie, des phases critiques – je pense plus particulièrement aux mises à jour. Comment ce problème est-il géré ? L'est-il de façon sûre ?

M. Gérard Berry. Ce problème a beaucoup évolué ces derniers temps. Par exemple, ceux qui possèdent un ordinateur reçoivent des nouvelles versions de logiciel – notamment du logiciel Java, qui, en ce moment, fait l'objet de nombreuses attaques. Avant, ce n'était pas le cas.

Mais ce qui vaut pour les ordinateurs est beaucoup plus compliqué pour les voitures. Je connais quelqu'un qui a acheté une voiture très moderne. Sous le capot de celle-ci, il y a des emplacements pour l'eau, l'huile, le lave-glace … et pour télécharger des logiciels. Or les garagistes sont très démunis devant les pannes logicielles. Dans cet exemple, le malheureux automobiliste est resté bloqué dans sa voiture ! Il faut combattre l'excès de maintenance. S'il s'agit de rajouter des fonctionnalités, pourquoi pas ? Mais si cela doit conduire à rajouter des bugs, c'est très dangereux.

M. Gilles Dowek. Une panne de téléphone risque de ne pas être bénigne. Le téléphone peut servir à appeler les pompiers. Au moment de la panne d'Orange, un seul réseau était affecté et on imagine qu'il aurait été possible, en cas d'incendie, de passer par un autre opérateur. Mais prenez le cas d'une personne attachée à la sûreté d'une centrale nucléaire qui utilise son téléphone lorsqu'elle est d'astreinte. Si un incident nucléaire intervient au même moment, il peut se produire des bugs en cascade, avec des conséquences tout à fait dramatiques.

M. Marko Erman. La société a évolué. Les réseaux de données nous offrent aujourd'hui des possibilités que nous n'avions pas par le passé, comme l'approvisionnement des grandes cités. La société devient donc extrêmement dépendante de leur bon fonctionnement.

Je suis d'accord pour dire que la panne d'un réseau de téléphonie ne peut être résumée à l'impossibilité de quelques personnes de communiquer. Elle peut aussi provoquer un « arrêt » de la société.

M. le président Bruno Sido. Cela relève d'une autre table ronde. Lorsqu'on a vraiment besoin de quelque chose, on doit avoir des systèmes redondants. Surveiller une centrale nucléaire avec un téléphone portable, ce n'est pas raisonnable ! Reste que le sujet est grave. C'est bien pourquoi, ce matin, j'ai parlé de « fragilisation ».

M. Gilles Dowek. Il n'y a qu'un seul réseau Internet. Celui-ci ne peut donc faire l'objet d'un système redondant.

Mme Nathalie Le Bars, du CEA. J’ai toujours un pincement au cœur quand on laisse croire que la sécurité nucléaire pourrait passer par un portable !

Mme Hélène Legras, correspondant « informatique et libertés » à la direction juridique d’Areva. En tant que salariée d’Areva, je confirme qu’on ne peut prendre un tel risque !

II. DEUXIÈME TABLE RONDE : L'INSTALLATION INSIDIEUSE D'UNE VULNÉRABILITÉ NUMÉRIQUE TOUS AZIMUTS.

Présidence de M. Jean-Yves Le Déaut, premier vice-président de l'Office

M. Jean-Yves Le Déaut, premier vice-président de l'Office. La première table ronde de l'après-midi était centrée sur le risque de système induit par la pénétration des outils informatiques dans tous les dispositifs de gestion et de pilotage. Ce risque de système a une dimension stratégique, car une paralysie globale de la société peut être la phase préliminaire d'une attaque militaire massive.

En 1943, René Barjavel avait imaginé le retour brutal au néolithique provoqué en quelques heures par une disparition soudaine de l'électricité. L'action de ce roman était censée se dérouler en 2052, mais notre dépendance à l'égard des systèmes numériques est déjà considérable. Notre deuxième table ronde a pour objet de montrer que la dépendance de système au niveau des outils de gestion se double d'un appétit collectif de consommation individuelle de services de communication numérique qui démultiplie les bienfaits mais aussi les risques. Il accroît en effet la fragilité intrinsèque de l'architecture sociale en cas de panne par un risque accru d'exposition à des attaques.

Les connexions individuelles à des fins personnelles, dans un contexte de proximité immédiate, ou même d'intégration, avec des outils informatiques de gestion, sont sources de failles potentielles dans les dispositifs de sécurité. Voilà qui explique l'idée directrice de cette table ronde, qui suggère l'installation insidieuse d'une vulnérabilité tous azimuts, à partir du constat du développement fulgurant des réseaux sociaux et des différentes formes du Web 2.0, qui fonctionne sur le principe d'une accumulation des données en ligne pour assurer des réponses plus rapides et précises.

Nous traiterons pour commencer de l'addiction aux systèmes numériques. Ce que certains considèrent comme un nouveau fléau crée des fragilités en raison du volume d'informations mis en ligne par les personnes concernées ; ces informations, qui concernent des individus et indirectement des organismes ou des entreprises, fournissent des points d'appui, au mieux à des ciblages aux fins de marketing, au pire à des attaques.

Nous aborderons ensuite les nouvelles formes de risques induits par le développement des réseaux sociaux. Là encore, le simple fait d'exposer sa vie publiquement, même de manière non pathologique, peut créer une faille de sécurité au profit de quiconque se donne les moyens d'analyser les informations. On peut d'ailleurs se demander si Facebook, Twitter – qui a fait son apparition à

l'Assemblée nationale – ou même Google ne sont pas des formes insidieuses de l'ancien réseau Echelon, si fortement critiqué en son temps.

Nous parlerons enfin des risques pour la vie privée de la dissémination des données numériques par les services en ligne, par les systèmes de télésurveillance ou de géolocalisation et par les objets intelligents. En 2009 déjà, la revue *Le Tigre* avait montré que l'on pouvait reconstituer tous les éléments de la vie d'un internaute pris au hasard. Les protections juridiques sont de moins en moins assurées en raison du nombre toujours croissant de données disséminées, majoritairement stockées sur des serveurs situés au-delà de nos frontières. Il paraît évident que la meilleure protection personnelle consiste en une hygiène individuelle d'utilisation des outils numériques, mais cela demande un grand effort pédagogique.

Nous entendrons d'abord le témoignage de M. Olivier Oullier, qui a enregistré son intervention, sur les axes de la recherche en matière d'addiction aux outils numériques.

M. Olivier Oullier, professeur à l'Université d'Aix-Marseille. Je vous remercie de me donner une nouvelle occasion de participer aux travaux de l'OPECST. Je souhaite préciser la notion d'« addiction ». Nous avons tendance à qualifier ainsi toute pratique excessive, toute consommation massive qui outrepasserait notre contrôle. Mais une utilisation extensive, même si ses effets sont délétères, n'est pas, du point de vue médical, forcément une addiction. Je ferai référence au *Manuel diagnostique et statistique des troubles mentaux* (DSM), publié par la Société américaine de psychiatrie et dont la cinquième version sortira en mai 2013. Lors des travaux préparatoires, qui ont duré plusieurs années, les auteurs du futur DSM-V n'ont pas éludé la question de l'addiction potentielle et des troubles liés à une pratique intensive de l'Internet, mais ils considèrent pour l'instant que les données disponibles ne sont assez probantes pour permettre de qualifier cette addiction de trouble psychiatrique. Les questions liées à cette pratique sont répertoriées en annexe du DSM mais pas, à ce jour, dans la partie principale, celle du diagnostic des troubles mentaux.

Dans l'étude *Cyberpsychology & Behavior*, publiée en 2008 et fondée sur des données recueillies entre 1996 et 2006, il y est dit en substance que certaines pratiques posent question mais qu'à ce jour la collecte des données souffre de biais dans le recrutement des sujets étudiés et que la définition même de l'addiction est problématique. Il faut donc poursuivre les études.

M. Allen Frances, professeur émérite à l'Université Duke, qui fut le président du groupe de rédaction du DSM-IV, a expliqué dans une tribune publiée en 2012, dans la version américaine du *Huffington Post*, pourquoi l'« addiction à l'Internet » était en train de devenir le nouveau concept à la mode, pointant la multiplication d'articles alarmants et de blogs arrachant des larmes, et l'apparition de protocoles de traitement à l'efficacité non démontrée – le marché explose car il

y a des millions de patients potentiels. M. Frances faisait observer que, sans aucun doute, nous sommes pour la plupart devenus « accrocs » à nos appareils électroniques et que certaines personnes s'en trouvent très mal, ayant un attachement malsain et incontrôlable à ces objets. L'important, poursuivait-il, est de « définir ce qui se passe pour pouvoir le traiter : que signifie le terme « addiction », et quand est-ce une manière utile de décrire nos passions et nos besoins ? Nous ne nous considérons pas « accrocs » à nos voitures, à nos télévisions, à nos réfrigérateurs… L'attachement à l'Internet est-il fondamentalement différent ? ». M. Frances observait encore que la définition donnée à l'« addiction » à l'Internet est très proche de celle que l'on applique à la toxicomanie, qui se caractérise par trois éléments : le besoin d'une consommation croissante ; le fait de se sentir excessivement mal quand on essaye de mettre un terme à celle-ci ; la consommation compulsive, presque sans plaisir et même si les conséquences en sont désastreuses sur les plans sanitaire, sanitaire, professionnel, personnel, financier et légal.

Sommes-nous esclaves de l'Internet ? Il faut distinguer le langage que nous utilisons tous les jours et la définition médicale.

Le DSM évoque les addictions comportementales, traite des jeux d'argent, des paris, et l'Internet est un candidat à la réflexion. Mais, avec les données recueillies à ce jour, les spécialistes ont été plutôt prudents et ils attendent de voir l'évolution et d'avoir plus de données.

Nos intérêts passionnés sont à risque pour certains : ils modifient nos comportements et peuvent nous isoler. Nous avons énormément d'exemples aujourd'hui, qu'il s'agisse de l'Internet et des réseaux sociaux ou de pratiques qui n'ont rien à voir avec cela. Il faut néanmoins rester très prudent et s'interroger sur les conséquences de ces comportements et, pour commencer, se poser la question de la pertinence qu'il y a à continuer de séparer comportements « réels » et comportements « virtuels », qui ne le sont plus du tout dès lors que les machines font partie de notre quotidien et induisent la mobilité et l'hyper-connectivité. Les chiffres sont ahurissants : plus de 340 millions de tweets sont échangés chaque jour ; il existe plus d'un milliard de comptes Facebook et 6 millions de vues par minute ; YouTube, présent sur plus de 350 millions de machines, propose 4 milliards d'heures de vidéo vues chaque mois pour un total d'un trillion d'heures visionnées en 2011. C'est un doux euphémisme de dire que nous avons une forte tendance à partager des informations… Pour beaucoup d'entre nous, c'est une pratique quotidienne.

La question est alors de savoir ce qui nous motive. Le plaisir, si l'on en croit une étude de Diana Tamir et Jason Mitchell, de l'Université de Harvard, publiée dans les Actes de l'Académie des sciences des États-Unis en mai 2012. L'étude a utilisé l'imagerie par résonance fonctionnelle magnétique, technique qui permet d'observer l'activité du cerveau et de voir si elle augmente de manière

significative pendant certaines pratiques. Il est apparu que lorsque les individus étudiés échangent des informations personnelles, l'activité du système dopaminergique mésolimbique – l'aire tegmentale ventrale et le noyau accumbens, autrement dit « le circuit de la récompense » – augmente de manière significative.

La série de cinq expériences réalisées montre que des gens préfèrent renoncer à une récompense sonnante et trébuchante pour pouvoir continuer à partager ces informations. C'est donc quelque chose d'extrêmement fort, qui s'accompagne de certains biais comportementaux, notamment une illusion de contrôle, d'immunité et d'impunité. Le fait que l'on ne se rende pas compte qu'en partageant des informations avec ce que l'on croit être quelques amis, on y donne en réalité accès au monde entier, qu'il s'agisse de nos « amis » ou de marques, d'institutions… à qui par le simple fait d'« aimer » et de partager, nous donnons un droit légal, très souvent, à l'utilisation de ces informations. Dès lors, des informations sensibles peuvent être partagées sans que les gens en soient conscients. On parle beaucoup de *big data* sans savoir réellement ce que cela implique, car il est très difficile d'évaluer les conséquences de ces nouvelles pratiques et de ces nouvelles collectes de données. Très peu d'études ont été rigoureusement menées à très grande échelle donnant des indications sur l'influence de ces réseaux.

Cependant, la revue *Nature* a publié en 2012 une étude réalisée par des scientifiques travaillant pour Facebook et portant sur 61 millions de personnes. L'étude a été menée pendant les élections au Congrès américain en 2010. À partir des envois sur le « fil d'information » de Facebook des incitations à aller voter, elle a montré l'influence qu'ont les personnes les unes sur les autres *via* les réseaux sociaux. On peut à cet égard s'interroger sur d'autres utilisations qui peuvent être faites de ce que l'on appelle l'influence des pairs, les nouvelles normes sociales transmises et diffusées par les réseaux sociaux.

Enfin, de nouveaux comportements bien réels émergent, qui sont rendus possibles par l'hyper-connectivité, la vitesse de transformation de l'information. On l'a vu avec les « printemps arabes », le mouvement des Indignés ou encore *Occupy* : se sont développées des révolutions sans chefs, une agrégation d'individus qui partagent des informations, l'émergence des « consciences virtuelles collectives » qui permettent à certains messages d'être portés. Mais comment ces mouvements se perpétueront-ils ? Un an ou dix-huit mois plus tard, on voit toutes leurs limites : certaines des idées ne sont plus coordonnées et l'on se rend compte de la limite de ces nouveaux comportements que, pour l'instant, on n'étudie pas encore assez.

On notera que, dans son *Global Risk Report* pour 2013, le Forum économique mondial a classé les « cyber-incendies sauvages » comme un risque majeur, qui peut avoir un impact sur la vie économique et sociale. On donnera pour exemple les rumeurs relatives à une banque française qui, s'étant propagées

sur Twitter et d’autres réseaux sociaux, ont fait plonger l’action pendant plusieurs heures.

Il faut prendre en compte l’ensemble des risques mais aussi des bénéfices – le fait que certains consommateurs ne soient plus isolés et que l’on crée des tactiques grossières de marketing. J’observe que ce sont souvent les spécialistes du numérique qui sont interrogés sur ces questions. Il est nécessaire – et je remercie l’Office d’envoyer ce message fort aujourd’hui – d’inclure dans vos travaux des spécialistes du comportement humain et des médecins. Il y a notamment énormément à apprendre de ce que l’on sait du fonctionnement du cerveau pour comprendre pourquoi les gens partagent des informations et pourquoi ils ont ce sentiment d’impunité et d’immunité. Les « comportements numériques » doivent être étudiés et enseignés dans les cursus des spécialistes du comportement humain et de la médecine, en coordination avec les spécialistes de la sécurité et des nouvelles technologies.

Je renouvelle mes remerciements à l’OPECST pour l’invitation qui m’a été faite et pour la considération ainsi témoignée à l’aspect comportemental, psychologique et neuroscientifique, très important dans ce qui est aujourd’hui une des questions primordiales du fonctionnement quotidien de notre société.

M. Jean-Yves Le Déaut, premier vice-président de l’Office. La parole est maintenant au Dr Marc Valleur, qui nous dira de quels éléments il dispose sur l’importance quantitative de cette forme d'addiction.

M. Marc Valleur, médecin-chef à l'hôpital Marmottan. Le scientifique qu’est Olivier Oullier et le clinicien que je suis envisageons le phénomène avec un regard différent, mais nous sommes d’accord sur l’essentiel. Si c’est de l’addiction aux jeux en réseaux sur l’Internet que l’on parle – une des formes d’addiction dont nous avons à connaître au centre Marmottan –, la prévalence de cette pathologie est infime. Parce que le consensus ne se faisait pas sur la définition de ce que serait une « cyberaddiction », nous avons constitué un réseau pour partager des cas cliniques avec des confrères suisses, belges et québécois ; sur une période de deux ou trois ans, nous sommes arrivés, ensemble, à identifier quelques centaines de cas. On voudra bien convenir que, rapporté aux millions de joueurs en réseau sur l’Internet, on est loin d’un raz-de-marée. Mais ce constat appelle d’autres questions : pourquoi un phénomène aussi mineur en nombre a-t-il une telle résonance médiatique mondiale ? Pourquoi est-ce sous l’angle de l’addiction que, très souvent, la question des jeux en réseau et d’Internet est abordée ?

Je tiens à souligner, plus nettement encore que ne l’a fait Olivier Oullier, que dépendance n’est pas addiction. Nous sommes tous dépendants de l’Internet comme nous l’avons été et le sommes de l’électricité, et comme l’humanité l’a été d’autres techniques auparavant. La dépendance peut être un phénomène tout à fait normal.

D’autre part, de faux consensus se forment autour du mot « addiction » car il a plusieurs significations. L’addiction clinique, celle dont on s’occupe quand, comme moi, on travaille depuis quarante ans avec des toxicomanes, des héroïnomanes, des cocaïnomanes, des joueurs d’argent, c’est le fait pour une personne de vouloir réduire ou cesser une conduite sans y parvenir, la perte de la liberté de s’abstenir.

En santé publique, l’addiction a un autre sens : c’est l’ensemble des dommages causés à la société par une conduite ou une consommation. Ainsi, l’immense majorité des quelque 40 000 morts dus chaque année à l’alcool en France n’a pas pour cause l’alcoolisme mais des accidents de la route, des violences ou des bagarres dont les auteurs ne sont pas alcoolo-dépendants.

La troisième acception du terme, c’est l’addiction au sens d’objet de l’addictologie. Pierre Fouquet, fondateur de l’alcoologie en France, définissait l’alcoolisme comme « la perte de la liberté de s’abstenir d’alcool » mais l’alcoologie comme l’étude de l’ensemble des relations entre les êtres humains et l’alcool, leurs aspects positifs pour l’individu et pour la société compris.

Autant dire que, contrairement à ce que l’on pense, on ne parle pas toujours de la même chose quand on parle d’addiction.

Quelle est la réalité clinique ? Les personnes que nous recevons à l'hôpital Marmottan viennent volontairement demander de l’aide pour cesser une conduite. Certains joueurs en réseau sur l’Internet se sont dirigés vers notre service après avoir appris qu’y était organisée une consultation « jeux », ignorant que par « jeux » il fallait entendre jeux d’argent ou de hasard, la consultation étant destinée à aider des gens qui se ruinent aux machines à sous par exemple. Si nous accueillons moins d’une cinquantaine de jeunes joueurs en réseau par an, nous recevons tous les jours des appels téléphoniques de parents affolés. Une inquiétude parentale considérable s’exprime donc pour une réalité clinique qui existe, certes, mais qui est, numériquement, extrêmement faible.

Ce que nous voyons se développer depuis deux ou trois ans et que nous essayons de freiner car nous n’avons pas le personnel nécessaire pour y répondre, c’est le problème des personnes qui demandent de l’aide pour arrêter de fréquenter des sites pornographiques ou de rencontres rapides. L’addiction sexuelle se répand dans la société par le biais des sites électroniques : ce qui avait commencé par être, en Amérique du Nord, une « maladie » de quelques stars ou personnalités célèbres se démocratise car l’Internet facilite l’accès à une sexualité mercantilisée. Ce qui est particulier dans notre consultation, c’est que, dans leur immense majorité, les personnes que nous recevons se masturbent devant les sites pornographiques mais ne passent pas à l’acte par le biais des sites de rencontres.

Ce ne sont évidemment pas les technologies de l’information et de la communication modernes qui ont inventé la masturbation, que Freud disait être

« l'addiction primitive ». Mais ce qui caractérise cette addiction masturbatoire assistée par ordinateur, c'est que comme pour beaucoup de pratiques actuelles, il y a un court-circuit direct entre la pulsion et le passage à l'acte : c'est une masturbation sans fantasmisation. Dans l'ancien temps, la masturbation était considérée comme un péché mortel, mais les théologiens avaient établi une gradation des fautes : le péché était mortel, soit, mais néanmoins relativement véniel si l'objet du désir était le conjoint légitime ; résolument mortel si le pécheur convoitait la femme de son voisin car il commettait alors, en plus, le péché d'adultère ; affreusement mortel car sacrilège si le fantasme portait sur l'image du Christ ou de la Vierge… Mais, dans le cas de masturbation assistée par ordinateur, on ne pense plus à rien : on regarde et on agit.

Ce court-circuit direct de la pulsion au plaisir explique peut-être pourquoi l'addiction est en passe de devenir le prisme au travers duquel nous sommes tentés de regarder tous les nouveautés qui arrivent dans la société – car ce mécanisme ne concerne pas que les sites pornographiques ou de jeux en réseau mais quantité de formes de consommation.

Ainsi, les problèmes d'addiction et de surendettement liés aux jeux d'argent ont commencé en 1987 avec l'introduction des machines à sous dans les casinos. On est alors passé de la loterie nationale, jeu de rêve où l'on imaginait ce que l'on ferait quand on serait millionnaire, à des jeux de sensation pure où l'on est hypnotisé par un écran. Cette recherche de sensation brute devient le mode dominant de consommation.

Les adolescents, dont on pense – peut-être à tort, comme le souligne le rapport de l'Académie des sciences – qu'ils sont des experts ès Internet, sont en réalité traités comme des cibles par les marchands, et ils ne s'en rendent pas compte. Il faut appuyer l'idée d'une éducation aux nouveaux médias, au décryptage des images par les adolescents. Quand on leur fait observer que Facebook et Google sont au nombre des sociétés les plus riches de la planète alors qu'elles ne leur proposent que des services gratuits mais dont ils ne peuvent plus se passer, et quand on leur demande ce que peuvent bien vendre ces entreprises pour accumuler de si grandes richesses, ils se rendent compte que l'objet vendu est leur profil, et que leurs données personnelles serviront à cibler les publicités de la manière la plus précise possible ; alors, ils commencent à réfléchir. 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. Car un même objet, le jeu en réseau, peut être utilisé soit de manière enrichissante, soit de manière abrutissante, pour faire le vide et rendre son cerveau « disponible pour la publicité »…

La meilleure prévention de l'addiction au jeu en réseau, c'est le développement de la qualité des jeux. Plus ils seront intéressants et complexes, plus il faudra, pour jouer, utiliser son imagination et sa pensée, moins ils seront

addictifs, car on devient en général « addict » à des conduites répétitives. Mais ce qui est facile à dire est difficile à mettre en œuvre, et il faudrait rappeler les sociétés de production à leurs responsabilités. Certaines en sont conscientes : ainsi, le syndicat des éditeurs de logiciels de loisirs a mis en œuvre le système signalétique européen PEGI, mais ni les distributeurs ni les parents ne sont au courant ; il faudrait améliorer l'information. Vivendi, qui fabrique le jeu le plus addictif qui soit, travaille aussi sur ces questions. Il reste à interpeller Facebook et Google sur leur responsabilité sociétale.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Le deuxième thème de cette table ronde pourrait avoir pour intitulé « Les réseaux sociaux sont-ils un cheval de Troie exposant les points névralgiques de la société ? ». Il s'agit, plus positivement, d'examiner comment l'on pourrait mieux faire prendre conscience aux internautes séduits par la convivialité en ligne de leur part de responsabilité potentielle face aux risques numériques.

M. Stéphane Grumbach va nous faire prendre la mesure des progrès fulgurants de la pénétration des nouvelles formes de l'Internet dans nos vies.

M. Stéphane Grumbach, directeur de recherche à l'Inria. La révolution numérique a engagé nos sociétés dans des transformations durables, géniales, mais dont nous sommes incapables, à l'aube de cette nouvelle ère, de mesurer l'impact. Il suffit de retourner seulement dix ans en arrière – Facebook n'existait pas – pour comprendre à quel point le changement est rapide, diffus et peu anticipé. Il est difficile de prévoir tous les services qui apparaîtront dans la prochaine décennie, mais il est déjà clair que certains de ces systèmes balayeront progressivement nos anciennes organisations.

Avant toute chose, je voudrais préciser deux points concernant l'orientation des thématiques abordées aujourd'hui. Cette journée est consacrée aux risques du numérique, non à ses opportunités. C'est une particularité européenne de voir dans la société de l'information avant tout une menace. Il en va vraiment différemment aux États-Unis ou en Asie, même si, bien sûr, le risque est un sujet pris très au sérieux et abondamment abordé aux États-Unis, en particulier ces derniers jours.

Ensuite, le sujet traité cet après-midi est intitulé : « Prémunir la société contre le risque de la dépendance numérique ». J'ai eu certaines difficultés à préparer mon intervention pour y répondre, car la question, dans le domaine de la toile et des réseaux sociaux, ne me semble plus être de prémunir la société contre ce risque : nous sommes déjà dépendants ! Elle est de savoir si cette dépendance est problématique, si l'on peut en sortir, ou comment on peut l'aménager.

Il y a, fondamentalement, deux types de risques : le premier est lié à la société de l'information en elle-même ; le second, à la dépendance à une industrie

étrangère dont nous n'avons pas la maîtrise puisque nous sommes incapables de la développer chez nous.

Le premier type me semble devoir être considéré comme les risques associés aux « *utilities* » de nos sociétés – l'énergie et les systèmes de transports par exemple –, c'est-à-dire en association avec les bénéfices de ces *utilities*, que personne n'envisagerait de supprimer, malgré les inconvénients qu'ils présentent.

Un risque spécifique retient particulièrement l'attention des Européens : celui de la protection de la vie privée. Plusieurs choses méritent d'être dites à ce sujet. D'abord, l'attention portée à ce risque est beaucoup plus forte en Europe qu'ailleurs. Or les outils de la société de l'information sont surtout conçus hors d'Europe. Ils sont donc *a priori* moins respectueux de la sensibilité européenne.

À ce jour, on peut s'interroger sur l'impact des normes européennes de protection de la vie privée sur notre capacité à construire une industrie. On pourrait souhaiter que ces normes assez exigeantes aient le même rôle que les normes environnementales sur l'industrie automobile par exemple, et contribuent à définir une nouvelle génération de systèmes de la société de l'information qui s'impose au monde. Mais on n'en est pas là.

De plus, il est difficile, je l'ai dit, d'imaginer, à dix ans seulement, l'évolution de la société de l'information et de ses services. Il est possible que les normes de protection de la vie privée se renforcent beaucoup. Il est également possible qu'il en aille autrement, et que la mise en ligne, de manière assez facilement accessible, d'informations considérées aujourd'hui comme privées et sensibles – les informations médicales par exemple –, ne pose pas vraiment de problèmes aux générations futures. Quoi qu'il en soit, ces informations sont déjà accessibles par effraction, et il faut faire avec.

J'en viens à l'anonymisation des données. Anonymiser les données, c'est perdre de l'information et donc une capacité d'extraction de connaissances et de services. Ce matin, Jean-Luc Moliner a montré l'impossibilité légale pour Orange de prévenir ses clients des attaques que subissent leurs machines. Il y a un subtil équilibre entre la sensibilité de l'opinion et l'intérêt économique et sociétal dans cette perte d'informations. Les réseaux sociaux ont vocation à enregistrer leurs utilisateurs sous leur identité véritable. Cela a suscité, tout récemment, un fort débat en Allemagne. De toute façon, Facebook et Google sont capables de calculer la véritable identité de leurs utilisateurs, en particulier par des techniques de *crowdsourcing*, en faisant travailler certains utilisateurs pour valider les informations des autres utilisateurs. On ne peut donc négliger aucune hypothèse sur le rapport que l'on aura, dans le futur, à la vie privée numérique.

S'agissant du deuxième type de risques – la dépendance à l'égard d'une industrie étrangère –, il me paraît assez sérieux. D'abord, parce que la croissance de ce secteur nous touchera beaucoup moins que les régions qui sont au cœur de

ces industries. Ensuite, parce que notre influence sur la définition de la société de l'information de demain risque de rester assez marginale. Enfin, parce que cette dépendance risque de s'étendre aux nombreux services que l'on n'imagine pas aujourd'hui et qui ne manqueront pas de devenir, eux aussi, indispensables à brève échéance.

Quant aux réseaux sociaux, ils sont en pleine évolution et leur appellation même porte à confusion. Comme je l'ai dit ce matin, Facebook, pour citer le plus connu d'entre eux, est bien plus qu'un réseau social. C'est un outil qui devient incontournable parce qu'il est utilisé pour l'authentification en ligne pour l'accès à de très nombreux services. Plus généralement, Facebook permet à un acteur économique tiers d'héberger des pages sur les infrastructures de cette société et d'accéder aux informations de ses utilisateurs avec leur consentement. Depuis sa création, il a évolué : d'outil de stockage et de diffusion de données personnelles – le réseau social à proprement parler –, il est devenu un système d'exploitation complet de ces mêmes données. Facebook, d'une certaine manière, est l'ordinateur de demain.

Une des caractéristiques essentielles de l'évolution de la société de l'information est le rôle imprévisible des données associées à certains services, qui peuvent être utilisées par d'autres services qu'on ne soupçonne pas à l'avance. Le traitement des masses considérables de données produites aujourd'hui suscite à la fois l'engouement de l'industrie du numérique et l'intérêt des scientifiques, auxquels il pose de nombreux défis. Le potentiel d'extraction automatique de connaissances à partir de données fait l'objet de nombreux débats. Jusqu'où sera-t-on capable d'aller ? Certains pensent que des découvertes scientifiques pourront être faites automatiquement à partir des masses d'informations disponibles. Nous ne sommes en tout cas qu'au tout début des potentialités ouvertes par les données numériques.

L'exemple du moteur de recherche, qui est l'un des premiers gros systèmes de la toile, illustre bien ce rôle des données. L'ensemble des requêtes faites sur le moteur permet de dresser le profil de chaque utilisateur. Mais, au-delà des utilisateurs, les requêtes permettent de générer des connaissances très riches sur des populations. Google a démontré ce potentiel en 2003, l'année de la crise du syndrome respiratoire aigu sévère (SRAS) : le système *Google Flu* sélectionne les requêtes relatives à la grippe sur l'ensemble de la planète, dans toutes les langues, et permet d'établir une cartographie exacte de la grippe en avance sur le Centre de prévention et de contrôle des maladies (CDC) des États-Unis.

Tout moteur de recherche, comme d'ailleurs de nombreux autres systèmes de la toile, dès lors qu'ils jouissent d'une couverture raisonnable, ont ainsi le potentiel d'analyser des populations sous d'innombrables critères. Le spectre des applications est large, du commercial au politique, en passant par la santé publique, le moral de la population… Si l'opinion publique s'est principalement

focalisée sur le profilage individuel, il me parait évident qu'il y a beaucoup plus de potentiel dans le profilage des communautés, des habitants d'un pays ou d'une région et, plus généralement, de toute population satisfaisant un quelconque critère. Par ailleurs, si la publicité représente aujourd'hui plus de 90 % des revenus de ces industries, il est probable que sa proportion diminuera au profit d'autres activités, pour peut-être tomber finalement à la proportion qu'a la publicité dans l'économie globale.

Un autre type de système a fait son entrée sur la toile récemment : les cours en ligne. C’est un exemple particulièrement intéressant de l’analyse des données que l’on peut faire de manière indirecte. Accessibles à tous, ces systèmes offrent des cours de très grande qualité, associés à un matériel pédagogique. Il est évident qu'ils auront un impact sur l'enseignement traditionnel et démocratiseront l'accès aux cours des plus grands maîtres. Pour suivre ces cours, il faut s'inscrire en ligne, sous sa véritable identité ; diverses incitations rendront le contournement de cette exigence peu intéressant. Le modèle économique de ces systèmes est simple : l'extraordinaire banque de ressources humaines, très précisément ciblées, au moment où les pays développés feront face à un manque d'ingénieurs et de scientifiques. Comme pour le moteur de recherche, la valeur ajoutée pour l'entreprise est éloignée du service offert.

Bien sûr, l'impact sur de très nombreuses institutions traditionnelles sera très important. Les négociations récentes entre Google et les organisations de presse de différents pays européens seraient d'une autre nature si l'Europe disposait elle-même d'un moteur de recherche. On peut craindre que des négociations du même type suivront dans d'autres secteurs d'activités qui, comme la presse, subissent la société de l'information et ses nouveaux outils ou services au lieu de prendre pleinement part à leur construction et à leur maîtrise.

Les données sont stratégiques pour un pays. Elles permettent l’analyse statistique d’un nombre illimité d'aspects qui, pour une part, correspondent à ceux que suivent les agences de statistique comme l'Insee. Certes, les méthodes d'analyse sont très différentes. Mais les agences de statistiques devront les intégrer au risque d'être complètement déclassées car, d'une part, les technologies d'analyse des données se raffineront progressivement, d'autre part, les analyses de flux produisent des résultats en temps réel, et non, comme pour ces agences, avec un décalage important.

Un autre aspect me paraît essentiel : celui de l’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. On peut imaginer qu'à brève échéance la France n'aura d'autre choix que de faire de même. Le risque existe que certains services régaliens liés à l'identité des personnes doivent être confiés à de telles sociétés si l’État ne dispose pas d'outils efficaces pour l'identité en ligne ; on

pourrait imaginer que, demain, la carte nationale d'identité française soit délivrée par Facebook.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. La parole est à M. Serge Abiteboul. Il évoquera les pistes qui s'offrent à nous pour essayer de concilier les avantages incontestables de l'interpénétration des réseaux et de la vie réelle et les risques collectifs qu'elle suscite.

M. Serge Abiteboul, membre de l'Académie des sciences. Je commencerai par insister sur les bienfaits du développement des réseaux sociaux, dont le premier, comme l'a dit M. Oullier, est le plaisir. Les jeunes gens prennent un plaisir considérable à communiquer entre eux sur ces réseaux, et les personnes âgées, maintenant qu'elles ont à leur disposition des outils d'utilisation plus facile, se réjouissent de sortir par ce biais de leur isolement. Il faut souligner cet apport, sans se limiter à une approche par trop négative qui consisterait à ne décrire que les risques des nouvelles technologies. Il serait bon de garder à l'esprit que si l'économie californienne s'est développée à ce point autour du numérique, c'est parce que l'on en souligne, là-bas, les avantages, et que l'on essaye d'inventer de nouvelles fonctionnalités.

Mais nous sommes réunis aujourd'hui pour traiter des risques, et je dois avouer que la masturbation assistée par ordinateur ne figurait pas dans la longue liste de ceux que j'avais à l'esprit. J'évoquerai pour ma part l'atteinte à la vie privée, qui me paraît être l'un des plus graves.

Les réseaux sociaux récupèrent une masse de données pour mieux vous servir. Pour vous recommander un restaurant, mieux vaut connaître vos goûts, vos interdits alimentaires, vos problèmes de santé, le temps dont vous disposez, etc. Il se trouve que ces informations valent beaucoup d'argent et, en un sens, c'est tant mieux, car les opérateurs peuvent offrir leurs services gratuitement.

Plus insidieusement, les données collectées permettent de mieux vous cerner. Si quelqu'un est un tant soit peu visible sur Internet, la quantité d'informations explicites est considérable, et suffit pour reconstruire sa vie. Si on creuse un peu, on peut, au moyen du traitement des *big data*, récupérer encore davantage d'informations. L'« anonymisation » des données est très relative dès lors que l'on dispose de temps de calcul.

Le web est devenu un village global, il faut s'y résoudre. L'anonymat et la protection de la vie privée sont en retrait par rapport à ce qu'ils ont été, et la situation est pire que dans vos pires cauchemars. Les données sont recoupées par des systèmes connectés entre eux. Et, avec les objets communicants, il y aura de plus en plus d'informations disponibles : on saura quand et où vous allez, ou ce que vous achetez.

Alors, que faire ? On peut agir dans quatre directions.

Premièrement, la loi. En France, on est un peu mieux protégé que dans d'autres pays grâce à la loi « informatique et libertés », même si elle n'est pas suffisante. Il est ainsi très difficile de faire respecter un droit fondamental comme le droit à l'oubli, par exemple, à cause des contrats qu'on est obligé de signer pour accéder aux réseaux sociaux et que personne ne lit parce qu'ils sont illisibles. Ce faisant, on renonce à tout droit de regard sur ses données, qui deviennent propriété de Facebook ou d'autres. Ce genre de pratique n'est pas acceptable et le législateur a du pain sur la planche. La tâche est complexe, c'est vrai. De quel droit et de quelle juridiction relève un Français en voyage au Maroc qui, pour « twitter », utilise un système américain dont les serveurs sont probablement implantés en Irlande ? En tout cas, il y a quelque chose à faire.

Deuxièmement, le travail des associations de consommateurs, qui est plus facile à mener. Un réseau social ne vaut que s'il inspire confiance car la valeur réside seulement dans les données collectées. Dès lors, le consommateur dispose de l'arme absolue : le boycott. Ainsi, quand Instagram, filiale de Facebook, a voulu s'approprier, pour les vendre, les photos qu'elle mettait en ligne, il y a eu une levée de boucliers et l'entreprise a reculé. Les associations de consommateurs ont donc un pouvoir bien réel et les pouvoirs publics devraient les aider.

Troisièmement, l'éducation. Il faut apprendre aux usagers, jeunes ou moins jeunes, à se protéger, en enseignant l'informatique. Comment, sinon, faire comprendre les risques qu'il court à quelqu'un qui ne sait pas ce qu'est une base de données, une ligne de code, une application ou un serveur ? Les citoyens internautes ne doivent pas être des analphabètes.

Quatrièmement, la recherche. Il y a beaucoup à faire pour développer des outils de protection conviviaux, à la portée de personnes qui n'ont qu'une connaissance rudimentaire, voire nulle, de l'informatique, de façon à leur permettre de spécifier le niveau et l'étendue de la protection des données qu'ils souhaitent.

Je termine par un exemple inquiétant qui vient des États-Unis, où des employeurs ont demandé à des candidats à des postes chez eux de leur communiquer leur mot de passe Facebook. L'accès à des informations privées devrait être purement et simplement interdit. De tels comportements illustrent la nécessité de s'en tenir à un principe simple : les informations recueillies par un réseau social sont propriété de l'individu qu'elles concernent et personne ne devrait avoir le droit de les accaparer.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Depuis sa création en 1978, la Commission nationale de l'informatique et des libertés (CNIL) est au cœur de notre dispositif de protection de la vie privée. Mme Sophie

Nerbonne va nous expliquer comment la CNIL continue à exercer son contrôle malgré la profusion des dispositifs de stockage des données.

Mme Sophie Nerbonne, directrice adjointe des affaires juridiques, internationales et de l'expertise de la Commission nationale de l'informatique et des libertés (CNIL). Je reprendrai à mon compte la conclusion de M. Abiteboul : les données figurant sur les réseaux sociaux sont personnelles, privées ; elles appartiennent à l'utilisateur et ne devraient pas pouvoir être réutilisées. Or on en est loin puisque le modèle économique sur lequel reposent les réseaux sociaux consiste à les monnayer.

S'agissant de la protection juridique des droits des personnes, le constat est simple : le bateau coule. Les internautes sont moins bien protégés que dans la vie réelle. Les traces qu'ils disséminent partout sur des serveurs délocalisés sont réutilisées et il est de plus en plus difficile d'avoir juridiquement prise sur des intervenants mondialisés.

Le cadre national fixé par la loi « informatique et libertés », modifiée en 2004, est insuffisant. À cet égard, le projet de règlement européen sur la protection des données personnelles comporte deux avantages considérables. D'une part, il vise à renforcer le droit des personnes. Cette approche, spécifiquement européenne, reste très minoritaire. Cela étant, une société numérique est tributaire de la confiance qu'elle inspire, si bien que les États-Unis, même en l'absence de loi générale de protection des données, y sont très attentifs. D'autre part, le règlement européen créera les moyens juridiques de peser sur les grands acteurs du numérique que sont Google, Amazone, Facebook et Apple – regroupés sous le sigle GAFA.

Le projet en cours de discussion devant le Parlement européen donne lieu à des débats virulents dans la mesure où, la législation interférant avec le modèle économique, les pressions sont très fortes, et les outils juridiques dont nous disposons menacés.

Ainsi, il faut tenir bon sur les principes et les notions de base, c'est-à-dire la définition des termes « données à caractère personnel ». Certains considèrent, contrairement à l'ensemble des autorités de protection des données, à la Cour de justice des communautés européennes et au Conseil d'État, que des identifiants numériques qui ne reprennent pas les coordonnées matérielles telles que le nom et l'adresse n'ont pas à être protégés, en particulier l'adresse IP. Comme l'ensemble du système de protection des droits d'auteur repose sur ce critère, il doit évidemment faire partie des données personnelles.

Préserver le champ d'application de la loi, renforcer les droits mis à mal par la façon dont est recueilli le consentement à l'exploitation des données – il est difficile de l'exprimer ou de le refuser quand on exige de vous de lire un contrat long et quasiment illisible –, tel est le sens de l'action de la CNIL vis-à-vis de

Google. Elle mène, pour le compte de tous ses homologues européens, un travail d'investigation sur sa nouvelle politique de vie privée. Celle-ci consiste à agréger l'ensemble des politiques suivies pour la quarantaine de produits et de services offerts par Google, dans le souci d'offrir une meilleure visibilité, mais aussi de combiner tous azimuts l'ensemble des données collectées. Nous estimons que ces procédés ne correspondent pas à ce que la directive actuelle prévoit en matière de respect de l'information et de contrôle par l'utilisateur des données le concernant. Le bras de fer est engagé avec cette société au niveau européen, le seul pertinent.

Pour protéger la vie privée, il faut évidemment une autorité de régulation suffisamment forte, disposant d'outils modernes de régulation, et qui puisse s'appuyer sur des principes solides. Contrairement à l'optique américaine qui se fonde sur la *self regulation*, des codes de conduite sur lesquels les acteurs se sont mis d'accord, nous prônons un socle législatif qui serve de base à des codes de déontologie et à la concertation sur des points pratiques. Ainsi, nous négocions les conditions de recueil du consentement des internautes concernant les *cookies* de profilage rencontrés au cours de la navigation.

Le label peut aussi contribuer efficacement à la protection. Nous n'avons développé cet outil que dans certains domaines, en matière de formation ou d'audit de traitement. Mais il pourrait parfaitement être utilisé pour des services de *cloud*, d'externalisation des données. D'ailleurs, certains prestataires, dans leur offre, garantissent que les données ne sortiront pas de l'espace européen. La protection de celles-ci peut être une source d'innovation pour les entreprises et les inciter à développer des produits labellisés conformes aux règles européennes. Cette approche susceptible d'inspirer la confiance peut attirer des clients.

Toutefois, on ne peut pas se contenter de protection juridique : la CNIL en est consciente. C'est la raison pour laquelle toutes les garanties d'ordre technique ne doivent pas être négligées. S'agissant du droit à l'oubli, les *tags*, qui indiquent à l'internaute la durée de conservation en même temps qu'il dépose la donnée sur Internet, nous paraissent une piste intéressante.

L'éducation représente enfin pour la CNIL un axe stratégique, car elle entend accompagner les jeunes générations dans leur découverte des nouveaux outils.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Je laisse la parole à Mme Chloé Torrès, qui va nous exposer les avancées et les imperfections de la couverture des données privées à l'échelle internationale.

Mme Chloé Torrès, directrice de l'activité « informatique et libertés » au cabinet Alain Bensoussan. Les données à caractère personnel, on l'a déjà dit, sont dispersées partout. Lorsqu'on ouvre un compte Facebook aujourd'hui, elles sont hébergées aux États-Unis. Ensuite, elles voyagent partout dans le monde au gré des prestations de *cloud computing* : un jour, elles seront

hébergées sur des serveurs situés en Grande-Bretagne, le lendemain, elles se retrouveront en Inde.

Cela dit, il existe aujourd'hui un socle juridique substantiel qui permet de protéger les données à caractère personnel. Outre la loi « informatique et libertés », il y a la directive 95/46/CE sur la protection des données, et demain le règlement européen qui harmonisera le droit à la protection des données au plan européen. Il ne faut pas non plus oublier l'article 9 du code civil qui consacre le droit à la vie privée. Au-delà des frontières européennes, certains pays ont adopté des lois dans ce domaine : Singapour vient de le faire, la Nouvelle-Zélande aussi, à qui la Commission européenne a reconnu un niveau de protection équivalent au sien, et le texte en vigueur au Maroc est pratiquement le même que la loi française. On peut dire que le cadre « informatique et libertés » est devenu un standard mondial. Notre modèle s'impose progressivement au niveau international.

La protection des données se traduit par un droit, pour les personnes en cause, à la transparence, à l'information sur la façon dont sont utilisées les données. Et elles peuvent agir sur elles par le biais d'un droit d'accès et de suppression, bien qu'en pratique, ces droits soient souvent difficiles à mettre en œuvre.

Le vrai vide juridique, qu'il faut impérativement combler, c'est l'absence de droit de propriété. Beaucoup de plates-formes aujourd'hui revendiquent la propriété pure et simple des données à caractère personnel postées par les internautes. Dans ce domaine, l'intervention du législateur est indispensable pour créer un droit de propriété qui soit personnel, incessible et inaliénable. Il s'agit d'un enjeu majeur.

Par ailleurs, les moyens à disposition se développent. Des entreprises s'efforcent de mieux appliquer le socle juridique existant et de protéger plus efficacement les données de leurs salariés. On voit se dessiner une tendance, parmi les groupes internationaux notamment, à adopter une approche *privacy based design*. La dimension de protection des données et de la vie privée est intégrée dès la conception d'un projet. Les promoteurs veillent à la conformité de la nouvelle base de données avec la loi en s'assurant que l'information des personnes est garantie et que la protection des données est effective, en amont et tout au long de la vie du projet. Cette démarche, qui est au cœur du futur règlement européen, sera obligatoire dès qu'il aura été adopté.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. C'est au tour de Mme Hélène Legras, d'Areva, de nous expliquer comment elle sensibilise les salariés à leur comportement sur les réseaux de façon à réduire les risques pour l'entreprise.

Mme Hélène Legras, correspondant « informatique et libertés » à la direction juridique d'Areva. Je vous remercie de m'accueillir pour parler d'un sujet passionnant et d'un enjeu important, y compris au sein de l'entreprise. Le statut de salarié ne donne pas à l'employeur le droit de faire n'importe quoi avec les données personnelles de ses employés. M. Alex Türk, au moment de la révision de la loi « informatique et libertés », a eu l'idée de créer les CIL, les correspondants « informatique et libertés », qui représentent en quelque sorte la CNIL au sein des entreprises. Ils sont chargés de veiller à ce qu'elles soient en conformité avec la législation. La loi « informatique et libertés » m'apparaît comme le prolongement de la Déclaration des droits de l'homme et du citoyen.

Être le correspondant unique dans un groupe comme Areva, qui compte, dans le monde entier, 280 sociétés et 48 000 salariés, fait de moi une sorte d'entonnoir par lequel passent toutes les demandes. Si un opérationnel décide de constituer une base automatisée, il viendra me demander si les données qu'il collecte sont personnelles ou non ; si leur traitement est automatisé, la loi « informatique et libertés » s'appliquera et la base devra faire l'objet d'une déclaration dans mon registre CIL.

Les instances représentatives du personnel (IRP) et les syndicats aussi se posent des questions. Eh bien, ils s'adressent à moi parce que le groupe a organisé une communication autour de ma nomination ainsi que sur mes missions. Juriste ou informaticien, le CIL doit connaître son entreprise et se faire connaître d'elle. Protéger les données personnelles constitue un sacerdoce.

J'ai beaucoup aimé, monsieur Le Déaut, que vous parliez d'« hygiène » à propos de l'utilisation des réseaux – plutôt que de « gouvernance » ou de « conformité » –, dans la mesure où il s'agit de ne pas faire n'importe quoi avec les données personnelles des salariés.

Au sein du groupe Areva, lors des formations que je fais, je recommande aux opérationnels de ne pas collecter de données sensibles – ethniques, raciales, voire philosophiques. Un service de ressources humaines peut être enclin de consigner le motif pour lequel telle ou telle personne n'a pas été embauchée. Si elle n'avait pas le profil ou les compétences, soit, mais on ne peut pas, dans les commentaires, mentionner sa tenue vestimentaire ou une information qui serait discriminatoire. Il est important que le CIL mette en garde les opérationnels contre les risques.

Sur le site intranet de la direction juridique, j'ai mis en ligne de nombreuses fiches sur le CIL, la CNIL, les données sensibles ou personnelles, dans lesquelles je donne de nombreux conseils.

Il faut aussi animer un réseau. Le CIL d'un groupe de 48 000 personnes ne peut pas tout savoir, mais il doit disposer d'une cartographie, devenue obligatoire depuis la loi « informatique et libertés ». Je tiens donc un registre de toutes les

bases du groupe Areva et je sais où elles sont. Comme l'a fort bien dit Chloé Torrès, l'éparpillement provoqué par le *cloud computing* peut être dangereux pour la sécurité et la confidentialité. D'ailleurs, le fameux règlement communautaire dont on a déjà beaucoup parlé introduit la notification des failles de sécurité. Je travaille main dans la main avec le Responsable de la Sécurité des Systèmes d'Information parce qu'il est le premier à connaître ces éventuelles failles. C'est lui qui me dira si le *hacker* a pu avoir accès aux données personnelles des salariés. De même, j'informe de mes missions. Très longtemps, les IRP se sont demandé pourquoi nous ne faisions plus de déclaration à la CNIL. Je suis donc venue au comité d'entreprise parler de ma fonction. J'ai expliqué que je travaillais étroitement avec la CNIL, que je veillais à la protection des données personnelles et qu'elles ne soient pas conservées indéfiniment.

Ainsi, si l'on fait par exemple une enquête de satisfaction, je m'assure que les données collectées à cette occasion sont détruites dès qu'elle est terminée. Quand nous faisons appel à un sous-traitant, je lui fais signer à ce dernier un accord de confidentialité dans lequel il s'engage à détruire les données personnelles collectées une fois son enquête achevée et à restreindre l'accès à ces données aux besoins et personnes en charge de l'enquête.

Je veille aussi à faire respecter le droit des personnes. J'informe les salariés qu'on collecte leurs données en vue d'un traitement informatique, et leur indique l'usage qu'il en sera fait. De même, je veille au respect de leur droit d'accès, de leur droit à modification, voire à suppression, s'exerce. Un salarié qui a quitté le groupe Areva a le droit de vérifier que celles qui le concernent ont été supprimées. Je m'assure enfin que les données sont bien « adéquates », c'est-à-dire pertinentes et légitimes. Par exemple, l'article 9 du code civil accorde le droit à l'image à chaque individu. La photo est aussi une donnée personnelle et la loi « informatique et libertés » s'applique. Pour l'annuaire intranet d'Areva, les salariés se voient demander s'ils acceptent que leur photo y figure. Au moment de leur embauche, ils signent une autorisation, sur laquelle ils peuvent revenir quand ils le souhaitent.

Le règlement communautaire va consacrer le droit à l'oubli. Techniquement, il sera très difficile à mettre en œuvre mais il est indispensable.

Débat

M. Laurent Gouzènes, membre du conseil scientifique de l'OPECST. On n'a pas parlé des vols d'identité numérique. À l'occasion d'un mail censé être destiné à la banque, les données peuvent être détournées et les comptes vidés. Il est très difficile ensuite de prouver la fraude et d'être rétabli dans ses droits. De même, des usurpations complètes d'identité ont eu lieu sur Facebook, par duplication pure et simple de comptes, si bien que l'on ne peut plus distinguer le vrai du faux. Si les deux fraudes se conjuguent, la situation devient très critique

car, faute de preuve, vous n’avez plus de contact avec votre banque et votre vie professionnelle et privée risque d’être très perturbée. L’isolement peut être total.

M. Sophie Nerbonne. Vous avez raison de souligner ce risque, qui constitue, aux États-Unis, le principal problème. Se développe ainsi un marché autour des « nettoyeurs » du net qui veillent à l’« e-réputation » de leurs clients. La CNIL reçoit également des plaintes à ce sujet.

M. Jean-Yves Le Déaut, premier vice-président de l’Office. En préparant cette audition, je me suis immergé dans ce monde que je connaissais mal et j’ai détecté quelques anomalies qui mériteraient attention. J’ai ainsi vu la photo d’une conseillère municipale du Sud de la France, honorablement connue, utilisée pour illustrer des messages de nature très différente. Il y a aussi moyen, en jouant sur les liens, d’afficher des messages sur le mur Facebook d’un tiers.

M. Stéphane Grumbach. Ne faudrait-il pas envisager un service public de l’identité numérique ? Aujourd'hui, beaucoup utilisent leurs identifiants Facebook pour s’authentifier et accéder à de nombreux services, s’épargnant ainsi une gestion des mots de passe de plus en plus compliquée.

M. Jean-Yves Le Déaut, premier vice-président de l’Office. C’est une des suggestions sur laquelle nous allons travailler.

M. Gérard Berry. J’attire l’attention sur l’impossibilité concrète de mettre en œuvre le droit à l’oubli à cause des procédures de *back up* généralisées dans les entreprises. Y a-t-il une législation sur ce point ? N’oubliez pas que les informations ne se contentent pas de circuler : elles sont aussi reproduites en maints exemplaires.

Mme Chloé Torrès. Le droit à l’oubli, c'est-à-dire la possibilité de disparaître des réseaux sociaux, est technologiquement neutre : il vaut quel que soit le nombre de duplications. Il existe pour chaque donnée une durée de conservation légale qui varie selon sa nature. Lorsqu’un salarié quitte l’entreprise, elle doit archiver les données qui le concernent aussi longtemps que le prévoit la prescription légale. Au-delà, il doit y avoir destruction. Il y a là, à mes yeux, un vrai chantier à ouvrir, car cela implique de mettre en œuvre un plan d’action sur plusieurs années. Adopter en amont une approche *privacy based design* pour les nouvelles applications permettra de se mettre en conformité à l’avenir. Pour le stock, c’est une autre affaire.

M. Gérard Berry. On risque de se trouver dans la même situation que pour le droit maritime : il existe mais il n’y a personne pour le faire appliquer.

M. Serge Abiteboul. Tout est une question de coût. Si la traçabilité a été prise en compte dès le départ, il y a moyen de détruire l’information, mais il faut avoir gardé les pointeurs dessus. Techniquement, c’est lourd mais possible. Et cher.

Par ailleurs, il peut y avoir conflit entre les règles, par exemple entre la durée légale et l'exigence de destruction du propriétaire des données.

Mme Chloé Torrès. Pour demander et obtenir la destruction de ses données, il faut justifier d'un motif légitime. Les exigences d'un salarié ne sont pas sans limite. En revanche, il peut y avoir un conflit de lois quand des bases centralisées sont soumises à plusieurs législations nationales. Les groupes internationaux doivent veiller à adopter une politique de durée de conservation des données harmonisée, qui ne soit pas trop coûteuse. Plus le problème est pris en amont des projets, mieux c'est.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Vous paraît-il possible que les données soient stockées sur la toile pendant un temps limité ?

M. Olivier de la Boulaye. Certainement, puisqu'il existe des logiciels pour cela. D'ailleurs, des sociétés commencent à proposer des services sur mobile qui utilisent des données éphémères. L'enjeu est le coût et la finalité de la requête.

M. Laurent Gouzènes. Ne sous-estimez pas non plus l'impact économique de ces réseaux américains qui vantent et commercialisent des produits américains réglés grâce à PayPal, une banque américaine, et livrés par une messagerie américaine. Ce sont autant de richesses qui disparaissent chez nous. On peut voir dans ce système une sorte de taxe Internet, qui coûte à la France quelques dizaines de milliards par an, et se mesure aussi en dizaines de milliers d'emplois perdus. Ces réseaux constituent aussi une arme économique au service de leur pays.

Enfin, j'avais été stupéfait de voir qu'après les attentats du World Trade Center, tout Internet s'était arrêté : plus rien ne marchait. Une telle panne est-elle encore possible aujourd'hui ? Les DNS – les systèmes de noms de domaine – étant pilotés par les Américains, nous ne maîtrisons rien et l'Europe peut se retrouver entièrement paralysée parce qu'un avion a été précipité sur une tour en Amérique.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. On a posé le problème ce matin dans le domaine militaire et évoqué la gouvernance mondiale d'Internet.

M. Laurent Gouzènes. Même si elle ne saute pas aux yeux, la vulnérabilité de notre économie est bien réelle.

Mme Hélène Legras. Dans ce cas précis, le réseau a peut-être été victime de sa sur-fréquentation. Quand l'information de l'attaque des tours jumelles a été diffusée, les gens se sont tous connectés à Internet pour voir en direct ce qui se passait. Et le réseau s'est effondré.

SYNTHÈSE DE CLÔTURE PAR M. MICHEL COSNARD, PRÉSIDENT-DIRECTEUR GÉNÉRAL DE L'INRIA

M. Michel Cosnard, président-directeur général de l'Inria. C'est une lourde charge que de proposer une synthèse de quatre tables rondes qui ont rassemblé vingt-cinq orateurs et suscité de multiples questions. Je remercie ceux qui ont contribué à la richesse des débats, et souhaite que cette réunion en appelle d'autres du même type.

La première table ronde de la matinée, consacrée à la place du numérique dans la gestion de la menace stratégique, a proposé un état des lieux en matière de cybersécurité. Dans ce domaine, le nombre d'attaques augmente de manière exponentielle. M. Chauve a montré la gradation d'une menace, qui va de la simple revendication ou de l'affichage de messages sur des sites officiels, par le biais du hacking, jusqu'au cyberespionnage, voire au cybersabotage. Les attaques sont imputables à des empilements chancelants de technologies. La maîtrise technologique doit pouvoir s'appuyer sur la confiance pour qu'on puisse construire une politique industrielle.

M. Grumbach nous a alertés sur le fait que les questions de souveraineté s'étendent au domaine des données, notamment personnelles. Il juge important que la France et l'Europe disposent d'une stratégie de récolte et de stockage, afin d'exploiter et de transformer ces données.

M. Pailloux a expliqué la stratégie de réponse élaborée par l'ANSSI. Elle se développe selon trois axes : conserver la capacité de protéger les informations essentielles, renforcer la sécurité des informations globales, promouvoir la sécurité dans le cyberespace. Selon lui, il existe une « hygiène informatique » que chacun doit respecter.

M. Bockel a présenté les grandes lignes de son rapport d'information sur la cyberdéfense, domaine où des progrès importants ont été accomplis. S'il faut donner la priorité à ce secteur, on doit aussi renforcer la cybersécurité et définir une stratégie européenne. M. Bockel propose également de créer une cyberréserve citoyenne – pour mobiliser des citoyens sur le territoire national en cas d'attaque massive –, d'adapter la législation au problème de la cybercriminalité et de rendre obligatoire la déclaration d'incidents. La communauté nationale doit être sensibilisée à ces enjeux majeurs.

M. Rihan Cypel nous a informés que le Livre blanc sur la défense, en préparation, ferait de la cyberdéfense un sujet majeur de sécurité nationale, de protection des entreprises et de lutte contre la cyberescroquerie. Il a plaidé pour la

création de filières universitaires, en rappelant que les risques pouvaient aussi être considérés comme des opportunités économiques.

M. Latty a détaillé les mesures prises par le ministère de la défense dans le cadre d'un schéma directeur de cyberdéfense et de cybersécurité.

Au cours de la deuxième table ronde, consacrée à la fiabilité et à la sécurité numérique des systèmes d'armes, M. Brugère a rappelé les étapes d'une conception sûre : établissement d'une chaîne de confiance ; maîtrise des technologies critiques ; développement d'expertises pointues liées à la sécurité des systèmes de défense et des infrastructures critiques ; mécanismes de surveillance et de détection ; partenariats de confiance.

M. Terrier a développé la notion de conception sûre. Tous les objets embarquant aujourd'hui de l'intelligence, ils doivent, pour communiquer, disposer d'une capacité d'adaptation et d'ouverture ; de ce fait, ils sont plus fragiles face aux attaques, et leur conception est plus délicate. Il a plaidé pour la mise en place d'une ingénierie système et logicielle à partir de briques fiables, dont les capacités ont été démontrées formellement.

M. Ripoche a indiqué que les risques, qui dépassent le cadre des équipements, s'étendent aux composants logiciels et, par-là, aux armes de défense. Il a souligné l'importance de la dualité civil-défense pour coordonner les efforts de recherche. Il a aussi montré l'intérêt et la fragilité de l'interopérabilité des systèmes d'armes dans des alliances comme l'OTAN. Le risque est gérable, à condition d'y consacrer les moyens.

M. Moliner s'est intéressé à la sécurité des grands systèmes de communication, à l'heure où des milliards d'objets sont connectés à Internet et où explose le trafic de données. Disposer de réseaux fermés étant impensable, la confiance devient un enjeu essentiel.

M. Malis a rappelé le rôle majeur qu'ont joué les évolutions technologiques dans les grandes confrontations, des guerres napoléoniennes à la Seconde Guerre mondiale. La maîtrise industrielle et technique est indispensable. Il faut considérer que l'ennemi est intelligent et s'intéresser à sa doctrine, impératif que l'on sous-estime parfois dans le domaine du numérique.

M. Mallet a rappelé le caractère exponentiel des cyberattaques et l'aggravation de la menace, bien que des stratégies de défense soient en cours d'élaboration. L'échelle de la menace dépasse les limites habituelles de la guerre ou de la dissuasion. La capacité de certains États à prendre le contrôle d'infrastructures ou d'entreprises ouvre des espaces insoupçonnés. Des groupes non étatiques peuvent développer des stratégies pour utiliser ces failles et ces espaces, afin de mener des guerres asymétriques. Le monde numérisé offre cependant des outils pour résister. Même si nous sommes toujours à la merci d'un

Pearl Harbor numérique, nous devons collectivement construire notre capacité de défense. M. Mallet a présenté l'organisation du ministère de la défense, depuis la chaîne de commandement opérationnel jusqu'aux investissements humains et techniques. Enfin, il a rappelé la dimension sociale et citoyenne du problème, en reprenant la proposition présentée par M. Bockel de créer une réserve citoyenne de cyberdéfense.

L'après-midi a été consacré aux moyens de prémunir la société contre le risque de dépendance numérique. Au cours de la première table ronde portant sur la sûreté numérique dans la gestion courante, M. Berry a rappelé l'origine et l'importance des bugs, en insistant sur la formation. Il juge préoccupant qu'on ne réserve pas au génie logiciel la même place qu'au génie mécanique.

M. Erman a montré que la protection des données allait devenir une préoccupation de sécurité nationale, ce qui est déjà le cas aux États-Unis.

M. de la Boulaye a traité de la sécurité des données dans le cadre de la domomédecine.

M. Dowek a présenté des cas de dysfonctionnement des systèmes informatiques.

Quant à M. Bolignano, il a évoqué les travaux conduits dans le cadre de la preuve de programme.

Au cours de la dernière table ronde, portant sur l'installation insidieuse d'une vulnérabilité numérique tous azimuts, M. Oullier a distingué la notion d'addiction et celle de dépendance, en rappelant qu'il n'y avait pas lieu d'assimiler certains nouveaux comportements à des problèmes cliniques.

M. Valleur a étendu la réflexion aux jeux sur Internet. L'éducation et la formation apportent des réponses dans ce domaine. Le développement de la qualité des jeux en réseau est la meilleure prévention de l'addiction. On parle parfois de « *serious games* ». Peut-être faut-il être plus sérieux pour jouer en réseau, sans perdre de vue la dimension ludique.

M. Grumbach, qui s'interroge sur les transformations durables de la société, a posé le problème de la protection de la vie privée, envisagé dans le cadre des réseaux sociaux par M. Abiteboul. Celui-ci identifie quatre leviers pour agir : la loi, les associations de consommateurs, l'éducation et la recherche.

Mme Nerbonne a montré que les internautes sont moins bien protégés que les citoyens. La loi relative à l'informatique et aux libertés étant devenue insuffisante, un règlement européen est en cours d'élaboration, car chacun doit pouvoir s'opposer ou consentir à l'utilisation de ses données personnelles.

Mme Torrès a expliqué qu'il existe un socle juridique protégeant ces données. Elle fait appel au législateur pour qu'il remplisse le vide juridique concernant leur propriété.

À partir de l'exemple d'Areva, Mme Legras a réfléchi sur la protection des données concernant les employés et sur le rôle joué par le correspondant « informatique et libertés ».

Un débat s'est élevé ensuite sur le vol de l'identité numérique, qui peut justifier la création d'un service public de l'identité numérique.

Un des maîtres mots de nos échanges a été l'éducation, qu'il s'agisse de se doter d'experts en matière de sûreté, de sécurité ou de fiabilité, ou tout simplement de comprendre le monde. L'OPECST a encore beaucoup de travail devant lui !

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Au cours de cette journée, beaucoup de sujets ont été abordés. Le développement du numérique et les risques qu'il présente sont un sujet très vaste, dont ni l'État ni le Parlement ne doivent se désintéresser. Nous avons travaillé en amont de la législation et de la régulation, pointant la nécessité d'instaurer un contrôle, mais, pour avoir déjà travaillé ici sur la cybercriminalité en 2005, nous savons combien il est difficile de mettre en place des règles de droit dans un domaine international et dématérialisé. Des constantes apparaissent cependant au niveau national, notamment la nécessité de développer la formation et la recherche, en ménageant la dualité du civil et du militaire. C'est ce que fait Thales, sous l'égide de Prix Nobel de physique Albert Fert. Le soutien à la recherche, comme le rôle des associations et du citoyen, est un enjeu essentiel pour le législateur.

Je vous remercie.

EXTRAIT DE LA RÉUNION DE L'OPECST DU 26 JUIN 2013 PRÉSENTANT LES CONCLUSIONS DE L'AUDITION PUBLIQUE

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.