ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Jeudi
21 février 2013
Séance de 9 heures

Compte rendu n° 58

SESSION ORDINAIRE DE **2012-2013**

Présidence
de M. Bruno Sido,
Sénateur, Président de l'OPECST
M. Jean-Yves Le Déaut,
Député, Premier vice-président de l'OPECST
Mme Patricia Adam,
Députée, Présidente de la Commission de la défense nationale et des forces armées de l'Assemblée nationale
et **M. Jean-Louis Carrère,**
Sénateur, Président de la Commission des affaires étrangères, de la défense et des forces armées du Sénat

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

Première partie :

La place du numérique dans la gestion de la menace stratégique

Première table ronde : état des lieux en matière de cybersécurité

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 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 Times* [(2)] 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 [(3)], 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 [(4)], mais aussi les marchés économiques, comme le marché du pétrole – le piratage du *compte Twitter* d'un diplomate Russe [(5)] 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 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

---

[(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/

[(2)] " Hackers in China attacked the Times for Last 4 months" http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

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

[(4)] 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

[(5)] "Twitter Rumor Sparked Oil-Price Spike," by Nicole Friedman, WSJ.com, August 6, 2012: http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html

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 [(6)].

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 [(7)]. 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 [(8)]. 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 [(9)], qui sont les bases de la confiance sur les échanges numériques, ou 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 [(10)] ou en ouvrant un attachement ou un lien dynamique dans un e-mail, 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.

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

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

[(8)] "Huawei and ZTE pose security threat, warns US panel"

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

[(10)] 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"

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.

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 Shangaï – 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'empois 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.

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.

Deuxième table ronde : Fiabilité et sécurité numérique des systèmes d'armes

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 10^{16} 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 10^{21} ? 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 XX^{e} 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 intégrées 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 xvii^{e} 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 concentrations 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.

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. Certaines 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 inter-parlementaire : 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.

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.

L’audition s’achève à douze heures trente-cinq.

La séance est levée à dix-huit heures.

*

* *

Membres présents ou excusés

Présents. - Mme Catherine Coutelle, M. Jean-Yves Le Déaut, M. Joaquim Pueyo, M. Eduardo Rihan Cypel, M. Philippe Vitel

Excusés. - *M.* Ibrahim Aboubacar, M. Claude Bartolone, M. Sylvain Berrios, M. Daniel Boisserie, M. Philippe Briand, M. Jean-Jacques Candelier, M. Éric Jalton, M. Bruno Le Roux, M. Maurice Leroy, M. Alain Marleix, M. Philippe Nauche, Mme Sylvie Pichot, Mme Émilienne Poumirol, M. Gwendal Rouillard, M. François de Rugy, M. Michel Voisin