Audition de Guillaume Tissier, président de CEIS

Rapport d'information pour la Commission des Affaires européennes de l'Assemblée nationale sur les effets de la transformation de l'agence européenne ENISA sur l'architecture de la cybersécurité européenne, et les conséquences plus larges de l'adoption du paquet cybersécurité.

Rapporteur - Monsieur Eric Bothorel

A propos de CEIS

CEIS est une société de conseil en stratégie et management des risques qui intervient dans le domaine de la cybersécurité à trois niveaux :

- *<u>Stratégique</u> : études et conseil pour le secteur privé et le Ministère des Armées (CEIS est notamment titulaire de l'accord cadre portant sur la réalisation d'études stratégiques relatives à l'espace numérique et à la cyberdéfense) ;*
- *<u>Opérationnel</u> : missions de conseil en cybersécurité ; Cyber Threat Intelligence, grâce à un équipe associant à la fois experts techniques, géopoliticiens, linguistes ; entrainement opérationnel grâce à BlueCyForce, premier centre européen d'entrainement opérationnel créé par CEIS et Diateam en 2017 ;*
- *<u>Evénementiel</u> : CEIS co-organise le FIC avec la Gendarmerie nationale depuis 2013 en intervenant à la fois sur le fond (programme, préparation des contenus, animation…) et la forme (organisation logistique, commercialisation).*

1. **Que pensez-vous du « paquet cybersécurité » ?**

Le Cybersecurity Act *(règlement européen relatif à l'ENISA e à la certification des technologies TIC, n°2019/881*) représente une avancée importante, tant sur le **renforcement de l'ENISA** (dont le mandat actuel arrive à expiration en 2020) que sur la **création d'un système de certification européen**.

Sur le renforcement de l'ENISA, le texte répond en fait à deux exigences importantes :

- Le besoin de disposer d'une ENISA renforcée et permanente pour assurer correctement la sécurité des institutions européennes.
- Le besoin également de donner à l'agence un rôle plus important en matière de coopération, voire, dans certains cas limités, de coordination entre les Etats. L'Agence assurera notamment le secrétariat du réseau des CSIRTs nationaux institué par la **directive NIS** (n°2016/1148). L'objectif est de pouvoir mettre en réseau les compétences, et si nécessaire, notamment pour les pays les plus en retard sur le sujet, mettre à disposition des capacités opérationnelles.

Sur le volet « certification », le texte répond également à deux exigences essentielles :

- La sécurisation de la transformation numérique avec au cœur les objets connectés grâce à un système de certification soutenant le développement d'une approche « by design », c'est-à-dire ne concernant pas uniquement les produits de sécurité mais « distribuant » la sécurité dans l'ensemble des produits numériques ou intégrant du numérique dans un objectif de résilience ;
- La nécessité d'harmoniser à l'échelle européenne le cadre de certification pour favoriser le développement d'un véritable marché unique du numérique grâce à une norme commune permettant à une certification faite en France d'être valable dans un autre pays européen. Cela réduira d'autant les coûts et les barrières à l'entrée pour les produits et services européens. On constate en effet que le marché unique peine à voir le jour en matière numérique. Or il est absolument indispensable que nos acteurs du numérique, et notamment de la cybersécurité, pensent non seulement aux Etats-Unis mais aussi aux autres pays européens dans leur stratégie internationale.

De façon globale, le Règlement fait partie de l'approche normative et réglementaire qui fait partie des leviers majeurs pour retrouver notre souveraineté numérique qui ne peut être qu'européenne. *Cf. citation de Lacordaire :* ***« entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime et la loi qui affranchit »****.* D'ailleurs, les Etats-Unis ont parfaitement pris conscience du risque et mènent un lobbying intense à Bruxelles pour tuer dans l'œuf ce volontarisme normatif européen… Ce règlement, à la suite du RGPD, de la directive NIS, du règlement eIDAS, constitue donc une formidable opportunité non seulement en matière de sécurité mais également au plan stratégique à la condition que l'on sache exploiter cet avantage pour promouvoir nos intérêts industriels et commerciaux de façon pro-active, en instituant une réelle préférence communautaire, et pas uniquement pour les solutions et services les plus critiques. Il devrait par exemple être institué un mécanisme de crédit d'impôt pour tout achat de solution française ou européenne dans certains domaines clés.

A propos de la notion de « souveraineté numérique »

La souveraineté étatique a considérablement évolué au cours des siècles. Avec la mondialisation, elle s'est progressivement diluée au profit des individus, des entreprises et des organisations internationales. S'il n'est pas l'unique responsable de ce phénomène de dilution, l'émergence du cyberespace l'a considérablement accéléré depuis 20 ans (territoire physique vs. territoire virtuel), d'autant que les Etats ont largement ignoré, au départ au moins, cette transformation numérique (certains diront que c'est d'ailleurs la raison du succès d'internet…).

La souveraineté étatique est donc désormais partielle et surtout partagée, mais elle n'en reste pas moins l'un des garants de la paix et de la stabilité internationale, les Etats restant les seuls sujets de droit international. Il est donc tout à fait légitime que la France et l'Europe entendent aujourd'hui défendre, voire retrouver, leur « autonomie stratégique » qui seule leur permettra de défendre leurs intérêts, à commencer par une vision du cyberespace protectrice des droits de l'individu.

Il faut donc aujourd'hui mobiliser tous les leviers pour retrouver des marges de manœuvre. Ces leviers (humain, technologique, fiscal, juridique et normatif, diplomatique, militaire) doivent nous permettre de compenser une faiblesse géopolitique et démographique : la taille de notre marché intérieur national. C'est pour cela que cette souveraineté ne peut s'entendre qu'au niveau européen, avec toutes les difficultés que cela comporte mais aussi avec tous les atouts du « vieux continent ». ***Non seulement, on a du pétrole (les données) mais aussi des idées…***

2. Quels sont selon vous les grands enjeux de la cybersécurité à l'heure actuelle ? Quelles menaces vous paraissent particulièrement préoccupantes, et quelles réponses doit-on leur apporter ?

Les grands enjeux de la cybersécurité sont tout d'abord **opérationnels** : pas de transformation numérique, pas de nouveaux usages, sans confiance, et pas de confiance sans sécurité…

Mais ils sont également **stratégiques** si l'on souhaite pouvoir préserver notre liberté de choix et ne pas se voir imposer des solutions et surtout des modèles qui ne nous correspondent pas forcément. Et nous sommes tous concernés : individu, entreprise, Etat…

Côté « menaces », il faut insister sur deux choses :

- Les **menaces qui sont susceptibles d'affecter le fonctionnement même d'internet**. Le réseau est devenu une véritable « commodité ». On oublie un peu rapidement qu'il ne fonctionne que grâce à un ensemble d'infrastructures, de câbles et de protocoles comme BGP ou DNS. Or ces infrastructures sont régulièrement l'objet d'erreurs ou d'attaques qui montrent leur fragilité. Il faudra donc investir pour que ces infrastructures résistent et répondent à la demande en matière de débit et de latence.
- Les **menaces visant les données**. Parce qu'elles sont le nouvel « or noir », elles sont des cibles attractives et relativement faciles. Et l'avènement du « cloud computing » n'a rien résolu du tout.

Certes, il peut permettre d'améliorer la sécurité au plan technique en mutualisant les efforts, mais n'est pas forcément synonyme de « confiance ». Il conduit en outre à une concentration des données relativement dangereuse. D'où l'intérêt des stratégies multi-cloud et du edge-computing en qui certains voient l'avenir…

Face à ces menaces, les réponses sont de deux ordres :

- Le développement de **l'intelligence artificielle (IA).** Il est essentiel pour améliorer nos capacités de détection mais aussi de réponse à incident en favorisant l'orchestration voire l'automatisation de certains processus. Pour des raisons d'auditabilité et de responsabilité, il faut en revanche que l'Humain reste dans la boucle…
- **L'investissement dans l'Humain**. Au-delà de la sensibilisation, il faut renforcer la formation pour disposer à la fois de développeurs maitrisant le sujet mais également d'experts, techniciens ou ingénieurs. La formation professionnelle et l'entrainement régulier doivent de ce point de vue jouer un rôle clé. C'est la raison pour laquelle nous avons développé notre centre d'entrainement opérationnel, **BlueCyForce**.

3. Quels sont aujourd'hui les principaux défis rencontrés dans le domaine de la certification ? Le système multi-niveau établi par l'Acte de cybersécurité vous parait-il adapté ?

Les défis sont nombreux :

- **Le premier** repose sur le **caractère volontaire du dispositif**. C'est un choix délicat. Mais c'était le seul possible. Il était en effet difficile d'imposer brutalement des schémas obligatoires sans risquer de freiner l'innovation et le développement du numérique. Le texte comporte donc un dispositif à double détente, avec des schémas qui seront dans un premier temps basés sur du volontariat, mais pourront ensuite devenir obligatoires. Cela initie donc un cercle vertueux, à la condition que l'on parvienne à faire adhérer au dispositif l'ensemble de l'écosystème (fabricants, consommateurs et autorités).
- **Le second** est d'avoir **des schémas qui « collent » aux réalités techniques et business**. Sans cela, ils ne seront pas utilisés et ne seront qu'une surcouche inutile. Il faut donc partir des travaux existants au sein des organismes de normalisation (ISO, CEN/CENELEC, ETSI…), des fédérations professionnelles, des associations de consommateurs etc. L'objectif est de trouver un compromis entre le besoin d'élever le niveau de sécurité et le modèle économique des produits. Tout le monde comprend que l'on ne peut pas ajouter 3 ou 4 euros de sécurité sur des produits vendus à 1 euro… Par ailleurs, il faut aussi s'inscrire dans des contraintes de « time to market » qui interdisent parfois des temps de certification trop longs…
- **Le troisième** concerne le **périmètre des schémas**. Il faut certifier des éléments constants et certifiables. Il faut en effet tenir compte de la rapidité du progrès technologique et de la vitesse des cycles de développement. Par ailleurs, en matière logicielle, il est tellement facile et rapide de mettre à jour un équipement que la certification ne constitue pas une garantie absolue… L'idéal serait bien sûr une sorte de certification continue mais cela est bien sûr difficile.
- **Le quatrième** concerne **l'harmonisation des pratiques d'évaluation**. Il est indispensable que les méthodes d'évaluation soient appliquées partout avec le même sérieux et que l'on évite le risque de dumping auxquels certains pays pourraient avoir la tentation de se livrer pour des

raisons économiques évidentes. C'est la raison pour laquelle la version finale du texte prévoit des « peer review » entre autorités nationales et accréditeurs.

Le système multi-niveaux est tout à fait adapté. Il est le seul permettant, au moins en théorie, d'élever le niveau moyen de sécurité de l'ensemble des produits sans pour autant faire niveler par le bas la certification, c'est-à-dire faire diminuer le niveau de sécurité des produits, services ou processus les plus critiques.

On ne doit pas confondre la simple conformité (la « case à cocher ») et la sécurité…

A chaque niveau, correspondent des exigences et des méthodes d'évaluation différentes : le premier niveau peut par exemple donner lieu à auto-évaluations, tandis que le niveau le plus élevé s'appuiera sur des tests d'intrusion. **La question se pose en revanche pour le niveau intermédiaire, dit « substantiel ».** Le risque est en effet de voir se développer une sorte de « **ventre mou** » regroupant les produits, services ou procédés que l'on ne peut pas qualifier de critiques mais qui ne sont pas non plus totalement anodins. Il faut absolument imposer pour ce niveau des tests dits de « résistance », qui peuvent être des tests en « boite noire » limités dans le temps, un peu sur le modèle de la CSPN française.

C'est le consommateur qui sera le « moteur » du système et son facteur clé de succès. Celui-ci commence à comprendre dans certains domaines que cybersécurité et sûreté de fonctionnement vont de pair**. Demain, aucun véhicule connecté ne se vendra sans que le consommateur ne soit convaincu du caractère sécurisé du véhicules**. Les constructeurs l'ont parfaitement compris et intègrent progressivement cette préoccupation à la fois au plan technique… et au plan marketing. La sécurité deviendra même un élément de différenciation, un avantage marketing. De notre côté, nous commençons à voir cette tendance positive à l'œuvre dans le cadre du Forum International de la Cybersécurité (FIC) que nous organisons. Alors que la plupart des utilisateurs finaux avaient la « sécurité honteuse » et considéraient il y a quelques années que parler du sujet revenait à exposer leurs faiblesses, certains comment à accepter de parler et de s'afficher sur ce thème.

4. **Estimez-vous le système de certification tel qu'il est proposé suffisamment ambitieux ? Pensez-vous qu'il faille aller vers un système plus contraignant ?**

Oui, le texte est déjà très ambitieux. Il prépare le terrain et donne un cadre pour l'élaboration des schémas. Ce n'est pas l'objectif du texte que de rentrer dans le détail des processus d'évaluation niveau par niveau ou des produits, services, et processus concernés. Cela laisse la place à la discussion.

Les schémas qui seront donc d'abord purement volontaires pourront ensuite, si la commission le décide, devenir obligatoires. Il est d'ailleurs précisé dans le règlement que la certification est volontaire, sauf si la législation européenne ou nationale ne dispose autrement. La commission doit en outre évaluer régulièrement, au plus tard le 31/12/2023 et au moins tous les 2 ans par la suite l'efficacité et l'usage des schémas de certification adoptés et décidé d'une liste des produits, services et processus couverts par un schéma de certification existant qui devraient être couverts par un schéma obligatoire. Le changement de statut n'est pas une décision à prendre à la légère. Le risque est de freiner la transformation numérique

en ajoutant des contraintes et des coûts supplémentaires dont pâtiront à la fois les offreurs européens et étrangers.

Mieux vaut donc quelques schémas bien faits, avec un processus participatif associant toutes les parties prenantes, plutôt que des dizaines qui ne serviraient à rien. Par ailleurs, il est clair, vu ses ressources que l'ENISA ne pourra pas produire des dizaines de schémas du jour au lendemain. Il s'agira de commencer par certains domaines où les travaux sont déjà bien entamés comme les objets connectés (plus d'une 20aine de schémas existent déjà…), les véhicules connectés, le cloud computing…

Le processus fonctionnera aux conditions suivantes :

- Les fournisseurs de produits, services et processus doivent s'approprier et adhérer au système. Il faut donc un processus « bottom-up » ;

- Le périmètre des schémas doit être défini avec soin. Certains seront sectoriels (le véhicule connecté par exemple), d'autres transverses (le cloud computing par exemple). Il faut surtout éviter que ne fleurissent des référentiels redondants.

- Un écosystème d'évaluation devra se mettre en place. Côté français, les actuels CESTI ne suffiront clairement pas à la tâche. Certains spécialistes de la conformité devront également intervenir, surtout pour le niveau élementaire.

5. **Comment pensez-vous que celui-ci s'appuiera sur les acquis existant en matière de certification ? Peut-on craindre un nivellement par le bas au regard des dispositifs de certification français ?**

Le risque de nivellement par le bas semble écarté compte tenu des modifications qui ont été faites par rapport à la version initiale du texte proposée par la Commission.

Le texte préserve en effet les 2 principaux acquis :

- L'existence de schémas qui ont prouvé leur efficacité comme le SOGIS-MRA pour le niveau le plus élevé. Celui-ci devrait ainsi être le premier schéma qui sera lancé par l'ENISA et donc européanisé, ce qui est déjà un défi en soit puisque l'accord ne concerne aujourd'hui que 14 pays…

- La forte expertise de certaines agences comme le BSI ou l'ANSSI en matière de certification. Leur rôle dans le processus est aujourd'hui garanti au travers de leur présence dans le European cybersecurity certification group (GECC), de l'accréditation des organismes d'évaluation, du contrôle de conformité qu'elles réaliseront pour les certificats et de la délivrance des certificats qu'elles assureront elles-mêmes pour le niveau d'assurance élevé, voire, dans certains cas, de moindres niveaux.

Ce que l'on peut craindre, en revanche, c'est que la France arrive en ordre dispersé pour défendre des schémas qui soient conforme à ses intérêts… Nous devons être force de proposition et harmoniser nos positions avant de les porter au niveau européen. Ces schémas représentent en effet un enjeu important

dans certains secteurs industriels. On peut citer par exemple : le véhicule connecté, le domaine naval, les objets connectés, les systèmes industriels etc.

6. **Pensez-vous qu'il soit opportun de renforcer le mandat de l'ENISA ? La structure de gouvernance proposée vous parait-elle pertinente ?**

Oui, ce renforcement était devenu indispensable. Davantage pour des raisons de politique industrielle et de stratégie internationale que pour des considérations techniques et opérationnelles franco-françaises. Nous avons en effet en France une agence remarquable qui constitue avec le BSI allemand la pointe du fer de lance de la cybersécurité européenne, et ce n'est pas faire injure à l'ENISA que de considérer qu'avec un budget d'à peine plus de 20 millions d'euros demain, ils ne pourront pas devenir une agence supranationale, ayant la haute main sur la cybersécurité de tous les Etats membres.

L'objectif est davantage de faire de l'ENISA une sorte d'agence « plateforme » permettant la mise en réseau des expertises européennes à travers un mécanisme de « pooling & sharing », animant les travaux de certification, organisant des campagnes de sensibilisation et des exercices réguliers, développant le « capacity building », produisant des études. Cela n'exclut cependant pas, comme le stipule l'article 7, à l'Agence d'intervenir de façon opérationnelle et de porter assistance, sur demande d'un pays.

7. **Comment envisagez-vous la collaboration du secteur des entreprises du numérique avec une ENISA renforcée ? Comment analysez-vous le système actuel ? Quel est aujourd'hui le rôle du secteur privé dans l'établissement des schémas de certification, et comment la nouvelle législation européenne va-t-elle le modifier ? Quelles seraient selon vous les moyens d'améliorer les collaborations à l'échelle européenne entre les organismes publics et le secteur privé ?**

La collaboration des entreprises sera organisée autour de groupes de travail ad hoc pour chaque schéma candidat et le « stakeholder cybersecurity certification group ». Nous pourrions d'ailleurs tout à fait, dans le cadre des prochains FIC, organiser des réunions de ces groupes de travail en marge de l'événement. Pour augmenter les chances de parvenir à rassembler les interlocuteurs nécessaires, notamment côté industriel, il s'agit en effet de massifier les choses. Or ces acteurs sont pour la plupart déjà présents au FIC. Mais le premier travail, en amont, consistera à harmoniser nos positions au niveau national. Il serait également intéressant de mettre sur pied un observatoire du marché européen afin de disposer d'éléments fiables sur l'évolution du marché de la cybersécurité et ses principales tendances. C'est d'ailleurs l'un des considérants du règlement (le 42).

8. **Quelles sont les actions menées par votre organisation en lien avec l'ENISA ? Pouvez-vous notamment revenir sur l'organisation de Eurocybex ? Quels enseignements ont-ils été tirés de cet exercice, et quelles suites ont-elles pu lui être données ?**

Les actions de CEIS en lien avec l'ENISA sont doubles :

- **Via notre filiale européenne basée à Bruxelles**, nous sommes prestataires de l'ENISA dans le cadre de prestations d'étude. Nous avons mené en 2018 une première étude sur le paysage des CSIRTs européens et sommes en train de boucler une seconde étude sur les « Incident Response Capabilities ». Nous avons par ailleurs été sélectionnés pour 4 contrats cadre sur le rail, l'énergie, le maritime et la santé.
- **L'ENISA est également partenaire du Forum international de la cybersécurité (FIC).** C'est pour nous essentiel puisque l'internationalisation de l'événement est l'un de nos objectifs stratégiques. L'Europe a en effet besoin d'un événement international lui permettant de développer à la fois son empreinte intellectuelle sur le sujet et son empreinte « business »…

Concernant l'exercice **Eurocybex**

Eurocybex est un exercice de cyber crise européen impliquant plusieurs Etats membres que nous avons coordonné en septembre 2011 dans le cadre d'un projet européen co-financé par la DG Home dans le cadre du programme CIPS. Les objectifs du projet étaient d'améliorer et de tester des procédures de coopération face aux cyber-crise de niveau européen. L'exercice avait à l'époque démontré combien la coopération interétatique, même au niveau européen, sur un sujet aussi sensible que les attaques informatiques devait commencer par des choses très prosaïques, comme la définition de procédures standard (alerte, communication, annuaire, outil de communication sécurisé etc.).

Quelles suites ?

Des exercices cyber sont maintenant régulièrement organisés par l'ENISA, y compris au plan opérationnel. Ces exercices illustrent l'importance de l'entrainement, et notamment de l'entrainement opérationnel en matière de cybersécurité. Nous pourrions là aussi organiser dans le cadre du FIC une journée d'exercice opérationnel dans un environnement de simulation technique ainsi que des formations à destination de pays européens demandeurs mais aussi de pays étrangers. Nous comptons prochainement le proposer à la Commission et à l'ENISA.

Le FIC en bref

Quelques chiffres :
- Plus de 10 000 visiteurs dont 1500 internationaux
- 400 partenaires privés et publics
- 15 000 m2 d'exposition
- 450 intervenants
- De nombreux challenges techniques et stratégiques

Le FIC 2020

- Passage de 2 à 3 jours avec 1 journée uniquement dédié au salon et 2 jours de conférences, ateliers
- De nombreux side-event dont l'ID forum sur les questions d'identité numérique, les Vauban Sessions (OTAN), Coriin (conférence sur l'investigation numérique)…
- Le thème : replacer l'humain au cœur de la cybersécurité

Les objectifs stratégiques
- Renforcer l'internationalisation (d'abord vers les pays européens)
- Mettre en avant l'innovation sous toutes ses formes (prix de la start-up, programme d'accélération…)
- Rassembler l'ensemble de l'écosystème (offreur, utilisateurs finaux, sphère académique, agences étatiques)
- Développer les partenariats avec les grands « utilisateurs finaux » afin d'intégrer au mieux la sécurité dans les différents secteurs d'activité (cela rejoint l'objectif de la certification).
- Rassembler à la fois les acteurs de la sécurité numérique mais aussi du numérique de confiance (cloud computing, identité…)

9. Le nouveau cadre européen vous parait-il de nature à renforcer la position européenne au niveau mondial ? Estimez-vous la gouvernance européenne sur ces sujets suffisamment lisible ?

Oui, ce nouveau cadre est intéressant pour renforcer la position européenne. Mais c'est un point de départ. Il faut ensuite que l'on se donne les moyens d'exploiter l'avantage que nous procure ce dispositif, tout comme le RGPD et les autres réglementations européennes, pour développer la filière européenne de cybersécurité et de numérique de confiance, notamment en matière de cloud.

10. Quelle est votre position sur les projets de création d'un réseau de centres de compétences européen en cybersécurité ?

C'est une excellente nouvelle ! Le développement du capital humain est essentiel en matière de cybersécurité (cf. le thème du FIC de cette année). De ce réseau dépendra aussi le succès du cadre européen de certification car il faut des experts pour créer ces schémas et ensuite les mettre en œuvre…

11. Quels défis sont aujourd'hui posés par le déploiement de la 5G à la cybersécurité ? Comment répondre selon vous de manière adaptée à ces enjeux afin d'accompagner les entreprises du secteur tout en protégeant les utilisateurs ? Quel rôle pourrait, selon, vous avoir l'ENISA, dans le déploiement de ce nouveau réseau ? Faut-il une stratégie européenne sur ces sujets mettant en jeu la souveraineté nationale ?

Quels risques ?

La 5G introduit deux éléments techniques nouveaux en comparaison avec les générations précédentes (2G/3G/4G) qui ont un impact sur la cybersécurité :

- Une architecture potentiellement « cloudifiable » qui a bien des mérites techniques mais accroit les risques de cybersécurité (éléments distribués, possibilités de faire tourner des applications sur des serveurs non propriétaires, OS ouverts)
- La multiplication des objets à connecter au réseau (en terme simple, c'est autant de points d'entrée dans le réseau et donc un risque plus important)

Nous devons donc faire face à deux risques :

⇨ Un risque de sécurité en termes de confidentialité des échanges mais aussi de disponibilité.
⇨ Un risque de souveraineté : « mettre dans le noir » un pays sera potentiellement plus simple, ce qui peut avoir des conséquences lourdes compte tenu de notre dépendance au numérique. Au-delà des enjeux économiques et industriels liés aux technologies 5G, c'est aussi la domination sur les usages et services que permettra la 5G qui est en jeu.

Comment répondre de manière adaptée ?

Il y a 2 niveaux de réponse :

- Une **réponse technique avec la certification de sécurité**. C'est donc le rôle de l'ENISA. Mais attention, ce n'est pas parce que l'on a une certification, que l'équipement est définitivement « secure ». Un logiciel sur un routeur se change en quelques minutes. Clairement, l'un des premiers schémas sur lesquels l'ENISA devrait travailler sera les équipements 5G. L'ENISA devra alors forcément s'appuyer sur le 3GPP. Ce ne sera pas simple d'harmoniser les positions mais la France peut jouer en la matière un rôle leader.
- Une **réponse de niveau juridique et politique concernant le niveau de confiance**. La confiance ne se décrète pas. C'est une notion subjective basée sur de multiples critères. En la matière, il faut par exemple demander aux fournisseurs d'équipement de réseau un certain nombre de garanties d'un point de vue gouvernance (états financiers audités, nomination des membres du board, structure du capital…), règles d'éthique, protection du travail etc.

Faut-il une stratégie européenne ?

Oui, comme sur tous les sujets stratégiques. Ce serait dommage d'abandonner Ericsson et Nokia…