ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Mardi
13 avril 2021
Séance de 10 heures

Compte rendu n° 57

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Michel Van Den Berghe, président de la mission Campus Cyber

La séance est ouverte à 10 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. M. Michel Van Den Berghe, directeur général d'Orange Cyberdéfense, est président du Campus Cyber. Notre mission s'intéresse à la cybersécurité et à la cyberdéfense, qui constituent en un sens le cœur de la souveraineté numérique. Nous les avons abordées sous plusieurs angles – la sécurité des systèmes d'information de l'État et des administrations publiques, l'adéquation entre l'offre cyber française et européenne et la demande des entreprises, en particulier pour celles qui ont des moyens limités, et enfin les enjeux de la formation, afin de conserver un potentiel d'innovation dans un secteur à fort contenu technologique.

Votre parcours fait évidemment écho, M. le directeur général, à ces différents sujets, puisque vous êtes à la fois le fondateur d'Atheos, entreprise de cyberdéfense rachetée par Orange, et président du Campus Cyber.

M. Philippe Latombe, rapporteur. M. le directeur général, je souhaiterais d'abord vous interroger sur la façon dont vous appréhendez la notion de souveraineté numérique. Il s'agit d'une question rituelle de cette mission, qui procède de la grande diversité des définitions existante. Que recouvre selon vous ce concept, que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle ? De quelle façon les politiques menées par les États peuvent-elles ou doivent-elles évoluer pour mieux intégrer cette composante stratégique ?

Je voudrais en second point revenir sur le Campus Cyber, évidemment, et sur les enjeux de formation attenants. J'aimerais que nous fassions ensemble un état des lieux de l'avancement de ce projet et que nous revenions sur ses principales spécificités. Je me demande également comment nos voisins européens s'organisent dans ce domaine. Très concrètement, disposent-ils de campus similaires ? Des coopérations ont-elles vocation à intervenir entre le Campus Cyber et d'autres structures d'États membres de l'Union européenne ? Enfin, je voudrais connaître le calendrier de déploiement de ce campus, et savoir quels objectifs vous vous fixez afin d'atteindre une taille critique pour peser dans ce domaine.

Enfin, je vous propose d'échanger sur l'écosystème des entreprises de cybersécurité et de cyberdéfense, dont Orange Cyberdéfense fait partie. Je pose à titre liminaire quelques questions pour lancer nos échanges, mais elles ont évidemment vocation à être plus larges. Comment jugez-vous le niveau de maturité de l'écosystème entrepreneurial français ? Les relations entre acteurs privés et publics en matière de cybersécurité et de cyberdéfense sont-elles suffisamment développées selon vous ? Comment pouvons-nous faire le maximum pour essayer de ne pas manquer les innovations qui pourraient se présenter dans ce domaine à l'avenir ?

M. Michel Van Den Berghe. Le premier grand point est celui de la souveraineté, qui consiste à maîtriser ses données et ses équipements informatiques, ce qui est particulièrement compliqué dans le contexte international des entreprises, pour deux raisons. La première est

qu'une grande partie des solutions utilisées ne sont pas françaises et souveraines. Par ailleurs, si l'on prend l'exemple du chiffrement, chaque pays possède ses propres normes, ce qui complique le partage des données. Nous insistons également beaucoup sur le fait que pour que les entreprises choisissent des solutions souveraines, il convient de porter ces dernières au moins au niveau des solutions américaines par exemple, afin qu'il n'y ait pas de freins à leur adoption.

C'est ce que nous voulons faire avec Orange Cyberdéfense : nous essayons de construire un leader européen, de nationalité européenne, si je puis dire, en expliquant aux grands clients internationaux qu'à expertise égale, ils ont le choix de confier le traitement de leurs données sensibles à un acteur européen.

Le Campus Cyber est un projet à l'initiative du président de la République. J'ai reçu une lettre de mission du Premier ministre en juillet 2019, me demandant d'examiner si l'écosystème français était prêt à se rassembler autour d'un seul lieu pour coopérer et partager les différentes informations dont il dispose, afin d'élever le niveau de cybersécurité de la nation et la protection des entreprises françaises.

J'ai remis un rapport au Premier ministre en janvier 2020, intitulé *Fédérer et faire rayonner l'écosystème de la cybersécurité*, et que vous pouvez retrouver sur le site de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Nous avions interrogé une quarantaine d'entreprises pour leur demander si elles étaient prêtes à venir travailler ensemble dans un même lieu, malgré leurs relations de concurrence. Nous avons également visité une dizaine de campus dans le monde (à Beer-Sheva en Israël, Skolkovo en Russie et New York), avons fait travailler les ambassades pour savoir ce qu'il se passait dans les différents pays.

On m'a demandé d'opérationnaliser ce Campus Cyber. En septembre 2020, le président de la République a acté deux décisions. La première est le lieu, qui sera La Défense, car 90 % des entreprises qui ont accepté de venir travailler dans cette structure ont demandé qu'elle soit localisée dans Paris intra-muros ou en très proche banlieue. Par ailleurs, la gouvernance de ce Campus Cyber sera réalisée par une société par actions simplifiée (SAS), détenue à 51 % par le privé et à 49 % par des capitaux publics.

Le président de la République a dévoilé, il y a à peu près un mois, le plan d'accélération cyber, auquel j'ai participé, annoncé ce Campus Cyber et les moyens qui lui seront donnés.

Nous finalisons en ce moment la phase de capitalisation privée : une soixantaine d'entreprises entreront au capital de cette SAS jusqu'au 15 avril. Nous espérons faire entrer environ 3,5 millions d'euros dans cette entreprise, avec un actionnariat qui sera représentatif de la mixité des différentes sociétés : il y aura de très grandes entreprises du CAC 40 et du SBF 120, les grands acteurs de la cybersécurité, mais également des petites et moyennes entreprises (PME), des entreprises de taille intermédiaire (ETI) et même des *start-up* et associations. Les tickets d'actionnariat sont de 100 000 euros pour les grandes entreprises, 30 000 euros pour les PME et 10 000 euros pour les toutes petites entreprises et les associations. L'État, par l'intermédiaire de l'agence des participations de l'État (APE), abondera pour entrer au capital à hauteur de 49 % de l'ensemble.

Nous créons un campus regroupant quatre grands écosystèmes, ce qui est unique dans le monde. Les entreprises déporteront une partie de leurs activités dans le Campus Cyber,

pour qu'il s'agisse d'un lieu opérationnel où des gens travailleront au quotidien. Elles sont incitées à y installer des équipes, qui ont tout intérêt à partager avec d'autres équipes, y compris lorsqu'elles appartiennent à des concurrents. L'exemple que je prends souvent est celui du village d'Astérix : les gens se disputent un peu sur le territoire, mais lorsque des ennemis viennent les attaquer, ils se rassemblent, prennent un peu de potion magique et luttent contre les pirates. Dans *Astérix*, comme vous le savez, les pirates se sabordent eux-mêmes quand ils voient arriver les Gaulois. C'est l'objectif que nous poursuivons. 2 000 personnes travailleront sur ce Campus Cyber. Nous avons déjà pré-vendu 1 900 postes. De nombreuses entreprises viendront positionner une partie de leurs troupes.

Le deuxième point est la recherche et l'innovation. La France est extrêmement performante en matière de cybersécurité. L'objectif de la structure est d'offrir un lieu permettant de continuer à être très innovant, et surtout d'industrialiser les innovations lorsque cela a du sens. La proximité avec les grands industriels aidera à accélérer les développements, qui pourront être mis à leurs catalogues. Nous créerons un laboratoire de recherche et d'innovation, des zones d'expérimentation et un espace d'amorçage et d'accélération de ce qui viendra de la recherche et de l'innovation.

La formation est également un sujet important. Nous souffrons d'un manque de ressources en cybersécurité. L'objectif est de rassembler plusieurs écoles pour pouvoir former plus de personnes dans le domaine : cinq à six écoles nous rejoindront. L'école pour l'informatique et les techniques avancées (EPITA) créera un bachelor dédié à la cybersécurité. Nous voulons également susciter des vocations. Nous ne manquons pas tant de formations, mais beaucoup de personnes pensent aujourd'hui que la cybersécurité est limitée à ce que nous voyons à la télévision, avec des geeks à capuche qui travaillent devant des écrans verts, alors que nous avons besoin de très nombreux talents pour nous accompagner.

La quatrième activité de ce Campus Cyber sera l'animation des projets communs. L'événementiel et les prestations en matière de cybersécurité seront réalisés sur ce Campus Cyber. Nous ne voulons pas constituer une galerie marchande ou un hôtel d'entreprises, mais faire en sorte qu'il y ait beaucoup de collaboration. 30 % d'espaces seront réservés par des acteurs privés, 15 % par des acteurs publics, 11 % seront dédiés à l'accélération (espaces « pépites », visant à aider les PME françaises à se développer, grâce à la proximité avec les grands acteurs internationaux ou les grands clients), 6 % à la formation et 35 % constitueront des espaces collaboratifs. Lorsque vous louez 10 mètres carrés d'espace personnel, on vous facture 13 mètres carrés, pour financer ces espaces collaboratifs.

L'augmentation de capital sera finalisée le 15 avril : l'entrée au capital de l'État par l'intermédiaire de l'agence des participations de l'État (APE) sera réalisée le 30 avril. Nous sommes également en train de finaliser la prise à bail avec le propriétaire de l'immeuble, qui devrait être effective le 30 avril, pour pouvoir démarrer l'agencement du Campus Cyber et lancer les groupes de travail afin de déterminer ce qui y sera fait.

En France, l'écosystème de la cybersécurité est très morcelé. On retrouve de grandes entreprises comme Orange Cyberdéfense, Atos, Capgemini, Thales, mais également une myriade de petites entreprises assez spécialisées. La grande difficulté est de trouver des ressources, de l'expertise dans ce domaine.

Des travaux ont été menés par l'ANSSI, qui a créé les opérateurs d'importance vitale (OIV), référencé un certain nombre de prestataires.

Les grandes entreprises commencent à avoir un niveau de sécurité leur permettant de se protéger contre certaines typologies d'attaques, ce qui n'est pas le cas des petites entreprises. Les ransomwares visant les hôpitaux, les administrations, les collectivités territoriales et les petites entreprises créent systématiquement des dommages très importants. Or, le métier de ces établissements n'est pas la cybersécurité. Nous devons trouver des solutions pour pouvoir les sécuriser de la façon la plus transparente possible, et amener de l'expertise chez eux. 66 % des PME qui sont touchées par un ransomware déposent le bilan. Je pense que les 30 % restant ont payé la rançon. Nous faisons un vrai constat d'échec sur la sécurisation des petites entreprises en France, qui nécessite une mobilisation pour les protéger au moins vis-à-vis des attaques basiques, du type des rançongiciels.

M. Philippe Latombe, rapporteur. Si nous revenons au Campus Cyber, avez-vous connaissance de projets similaires, y compris en gestation, dans d'autres pays européens ?

M. Michel Van Den Berghe. Non, nous sommes en avance sur le sujet. Nous avons cependant créé de l'envie, et je commence à être en relation avec des confrères en Italie, en Belgique et en Allemagne, qui estiment que notre projet est très intelligent et demandent que nous élaborions un kit de création d'un campus cyber. Pour l'instant, nous sommes vraiment en avance par rapport aux autres pays européens.

M. Philippe Latombe, rapporteur. Avez-vous des contacts avec la Commission européenne, pour essayer de faire de l'initiative quelque chose de plus européen et généraliste ?

M. Michel Van Den Berghe. Nous avons postulé pour constituer un *« European digital innovation hub » (EDIH)*, de sorte que le Campus Cyber puisse être annoncé comme un dispositif d'innovation européen. Nous sommes portés par la région Île-de-France dans cette démarche. Ce sera peut-être un moyen de nous faire connaître.

Je suis un entrepreneur et j'avance donc, pas à pas. La première étape était de créer cette SAS française et la capitaliser, en faisant en sorte que tous les acteurs aient leur voix dans la gouvernance. Malgré l'entrée au capital de grandes entreprises, j'ai tenu à ce que le conseil d'administration soit représentatif de l'ensemble de l'écosystème. Il y aura un siège pour les *start-up*, un pour les associations, un pour les personnes de la formation, un autre pour ceux de la recherche. Je suis en train de finaliser cette phase du travail.

Par ailleurs, lorsque l'on crée une entreprise, on ne prend généralement pas un immeuble de 26 000 mètres carrés. J'ai donc aussi pour tâche de rassurer le propriétaire de l'immeuble, qui est neuf, quant à la pérennité de la SAS et à sa capacité à payer ses loyers. Je travaille également à l'établissement des contrats de sous-location : sur 2 000 postes de travail disponibles, 1 920 sont d'ores et déjà pré-vendus, ce qui montre que l'écosystème répond présent. Certaines entreprises prendront un étage complet de l'immeuble, d'autres occuperont seulement un ou deux postes de travail, qui leur permettront de s'immerger au sein de ce Campus Cyber.

M. Philippe Latombe, rapporteur. Il est dit que le campus ne sera pas localisé uniquement à La Défense, mais qu'il essaimera en province. Avez-vous déjà un plan d'essaimage ?

M. Michel Van Den Berghe. Oui, nous avons rencontré l'ensemble des présidents de région. Certaines sont déjà en train de créer leur campus cyber, comme la région des Hauts-

de-France, qui l'a fait avec la métropole de Lille et la ville de Lille. Nous avançons en parallèle : ils démarreront leur structure dès 2022 également. Je suis aussi en relation avec la région des Pays-de-Loire, pour examiner comment ils pourraient démarrer un campus cyber dans leur pôle d'innovation. Chaque région a manifesté son intérêt. Nous tenons absolument à pouvoir le réaliser : nous devons pouvoir amener la cybersécurité aux endroits où se font les grandes transformations numériques dans le pays. La région Rhône-Alpes est par exemple très en pointe sur l'industrie 4.0 : un campus cyber dédié à ces transformations doit y être constitué. Dans les Hauts-de-France, nous voulions travailler sur la sécurisation de l'écosystème des PME et la mise en place de solutions les plus transparentes possible. Dans les Pays-de-Loire, le travail porte sur la sécurisation des *smart cities*. L'idée est d'amener le concept de campus cyber dans les régions, pour constituer des satellites communiquant entre eux, de sorte que l'on ne fasse pas un projet jacobin où toute l'expertise serait centralisée à Paris.

M. Philippe Latombe, rapporteur. Il s'agissait de ma question suivante, à laquelle vous avez commencé à répondre. Chaque nouveau centre régional aura-t-il une spécificité ou une thématique particulière et pourra-t-il communiquer directement avec les autres centres, sans nécessairement passer par le campus parisien ?

M. Michel Van Den Berghe. Exactement.

M. Philippe Latombe, rapporteur. Comment percevez-vous l'appétence des chefs d'entreprises et des élus locaux sur le sujet ? Sont-ils suffisamment informés des risques cyber aujourd'hui, ou reste-t-il de l'éducation à faire ?

M. Michel Van Den Berghe. Le risque cyber est considéré comme majeur dans les grandes entreprises : la prise de conscience est faite. On nous demande de plus en plus d'organiser de la sensibilisation, des exercices de gestion de crise, etc. Nous percevons que ce risque est aujourd'hui identifié, et nous nous faisons aider par les grandes compagnies d'assurance pour rappeler qu'en cas de risque cyber, les dommages sont assez importants. Une vidéo a circulé sur Twitter, diffusée par un maire qui a subi une attaque par un rançongiciel. Il notait que l'on a toujours l'impression de ne pas être concerné, et que les pirates ne s'intéressent pas à nous. Or, aucune municipalité n'est particulièrement visée : les pirates lancent l'attaque sur le réseau, et ceux qui ont les portes ouvertes laissent entrer le rançongiciel et se font encrypter leurs données, qui sont dès lors perdues, si elles n'ont pas été sauvegardées.

Dans l'automobile, la sécurité du véhicule est un critère de choix, sans que l'on demande aux utilisateurs de connaître le fonctionnement de l'ABS ou des airbags. Nous devons développer cette approche en matière de cybersécurité, par des campagnes de sensibilisation, sur le modèle des campagnes-chocs qui ont été menées en matière de sécurité routière. Il y a un vrai travail de sensibilisation à mener de la part de l'État, pour rappeler qu'Internet n'est pas le pays de Candy et que l'on est visible de tous et très fortement attaquable dès lors que l'on ne se protège pas. Il faut mener un vrai travail de sensibilisation, d'éducation, pour que les gens comprennent que le risque est avéré, et que l'on parvient très souvent, avec très peu d'investissement, à se protéger de 90 % des attaques.

M. Philippe Latombe, rapporteur. Pensez-vous que cela aille de pair avec le manque de candidats au suivi des formations et à l'entrée dans le monde de la cybersécurité ? Ce domaine n'est-il pas suffisamment attractif ? N'en parle-t-on pas assez ?

M. Michel Van Den Berghe. Vous avez tout à fait raison. La cybersécurité souffre d'un problème d'image. Nous avons une image anxiogène. Tous les reportages télévisés présentent des spécialistes de la cybersécurité avec des capuches devant leurs écrans, ne parlant à personne. Or, ce n'est pas du tout notre métier.

Lorsque nous intervenons sur des crises sensibles (celles des hôpitaux, celle de Pierre Fabre, etc.), nous sommes confrontés à une première étape de stupéfaction et de panique, les victimes pensant jusqu'à ce qu'elles soient atteintes qu'elles n'étaient pas ciblées. Nous aidons très souvent à calmer, à structurer la réponse et à éviter la propagation de l'attaque. Lorsque les pompiers interviennent sur un incendie, ils n'envoient pas de l'eau partout, mais coupent l'électricité, le gaz, s'assurent qu'il n'y a plus personne dans les locaux, etc. Dans une crise cyber, le réflexe est exactement le même. Dans une deuxième phase, nous essayons de faire fonctionner les systèmes du mieux que nous pouvons. La troisième phase est celle de la reconstruction.

Nous devons changer l'image des personnes de la cybersécurité, donner du sens à notre métier. Je pense qu'un jeune sur dix mille en terminale indiquerait vouloir travailler dans le domaine de la cybersécurité si on lui posait la question. Nous avons besoin de communicants, de personnes capables d'aider à reconstruire des systèmes d'information, de spécialistes du chiffrement de données, etc. Il existe de nombreux autres métiers que ceux de pentester ou de hacker éthique, que l'on cite très souvent. Nous devons changer l'image du métier de la cybersécurité. Nos grands dirigeants eux-mêmes, lorsqu'ils ont l'occasion de communiquer sur le numérique, préfèrent parler du quantique que de cybersécurité, car ils estiment que cela est moins anxiogène. Or, notre métier n'est pas anxiogène. Nous sommes les Casques bleus du numérique : nous devons protéger un territoire, protéger des personnes. Notre métier a beaucoup de sens, et nous devons le valoriser pour créer des vocations. Les formations existent, mais ne sont pas remplies ; nous devons faire venir les jeunes vers ces métiers de la cybersécurité, en changeant son image qui est aujourd'hui trop anxiogène.

M. Philippe Latombe, rapporteur. Ces métiers sont-ils pratiquement toujours tenus par des hommes, ou commence-t-il à y avoir des femmes ?

M. Michel Van Den Berghe. Des femmes commencent à y être présentes, surtout dans les équipes de conseil. Orange Cyberdéfense est par exemple passé de 8 % à 17 % de personnel féminin entre 2018 et 2020. Il reste beaucoup à faire, mais nous y travaillons, toujours en changeant cette image du monde de la cybersécurité.

M. Philippe Latombe, rapporteur. Nous avons parlé de formation initiale et d'attirer des jeunes, en changeant l'image de la cybersécurité. La formation professionnelle continue est-elle pour sa part suffisante afin que des directeurs des systèmes d'information (DSI) ou des responsables de la sécurité des systèmes d'information (RSSI) soient mis à niveau des menaces existantes, de leur évolution technologique, etc. ? Le Campus Cyber proposera-t-il des formations dans ce domaine ?

M. Michel Van Den Berghe. C'est exactement ce que nous souhaitons faire.

Les formations doivent, en premier lieu, mettre à niveau les professionnels de la cybersécurité par rapport aux nouvelles typologies d'attaque. Les pirates sont extrêmement créatifs, et chaque innovation crée de nouvelles fenêtres de vulnérabilité. L'Internet des objets (IoT) créera de nouvelles vulnérabilités. Si ces objets ne sont pas référencés et, un minimum, sécurisés lorsqu'ils seront connectés au réseau, ils constitueront des portes d'entrée

supplémentaires. La 5G créera également de nombreuses possibilités de connexions d'objets, et augmentera donc la vulnérabilité. Nous devons donc former les acteurs, ce qu'il est prévu de faire sur le Campus Cyber pour que les RSSI et les DSI soient mis à niveau.

Nous essaierons en deuxième lieu de réaliser du *rescaling* d'ingénieurs réseau, d'ingénieurs de production informatique, de développeurs, qui ont envie d'aller vers le métier de la cybersécurité. Certaines grandes entreprises ont monté leurs propres formations pour faire du *rescaling* de ressources : nous l'avons fait chez Orange, EDF l'a fait, de même que BNP. Plutôt que laisser chaque entreprise mener ce travail de façon artisanale en son sein, nous voulons structurer la démarche, en nous faisant aider, par exemple, par l'ANSSI, qui pourrait dispenser des formations. La formation de ce type de populations à la cybersécurité est très rapide.

Le troisième point est que beaucoup d'écoles d'ingénieurs forment à la cybersécurité, mais que nous avons également besoin de techniciens supérieurs dans ce domaine. D'où la création de ce *bachelor* avec l'EPITA, pour augmenter le nombre de spécialistes en cybersécurité. Lorsque vous placez des ingénieurs derrière des consoles de cyberSOC (le système qui permet de surveiller ce qu'il se passe sur les réseaux), ils partent après trois mois. Nous devons également former des personnes à bac+2 ou bac+3 en école d'ingénieur, pour que l'expertise ne se trouve pas uniquement chez des personnes titulaires d'un bac+5. Nous avons besoin de bac+2 pour installer des matériels destinés à la sécurité périmétrique dans les entreprises, paramétrer des sondes réseau, etc. C'est ce que nous voulons faire sur le Campus Cyber.

M. Philippe Latombe, rapporteur. Beaucoup de projets de *smart cities* démarrent actuellement, pour des raisons de calendrier – puisque les maires ont été élus l'année dernière. Intègrent-ils suffisamment la cybersécurité dès l'origine, ou s'agit-il d'une préoccupation qui émerge à la fin du projet ? De même, les PME et ETI qui développent leurs systèmes d'information intègrent-elles la cybersécurité dès le départ ? Si ce n'est pas le cas, comment faire en sorte que la cybersécurité soit à l'avenir prise en compte en amont des projets ?

M. Michel Van Den Berghe. C'est toute la problématique que nous essayons de traiter par le *secure by design*. La cybersécurité est toujours traitée à la fin des projets, et comme ces derniers sont toujours en retard, elle est fréquemment oubliée. Je suis intervenu à la suite des attaques des hôpitaux : quand on voit les « cochonneries » qui sont connectées aux réseaux de ces établissements, il ne faut pas s'étonner qu'ils subissent des cyberattaques. Il faut en premier lieu interdire la connexion à des réseaux sensibles d'outils, d'objets connectés, de systèmes d'information qui ne sont absolument pas protégés. Il convient également d'inculquer le *secure by design*, en expliquant aux fournisseurs de ces solutions que la cybersécurité est un facteur différenciant, et qu'à prix égal, un client préférera retenir une solution dans laquelle la cybersécurité a été pensée.

Nous revenons au fait qu'il s'agit d'un problème d'éducation et de sensibilisation. Si la cybersécurité est prise en compte à l'origine, le projet n'est absolument pas ralenti, au contraire, et les systèmes d'information ne seront pas complètement piratables.

On attaque aujourd'hui les données des entreprises. Dans cinq ans, les rançongiciels toucheront les particuliers : lorsque les maisons seront complètement connectées, on exigera des personnes qu'elles paient une rançon directement avec leur smartphone pour pouvoir ne serait-ce qu'entrer chez elles. De même, la numérisation des *smart cities* est une bonne chose, mais si le pirate prend la main sur une ville connectée, il est capable de faire n'importe quoi.

Il faut donc vraiment sensibiliser maintenant les personnes à prendre en compte le risque. Pour être très franc, ce n'est pas du tout fait aujourd'hui.

M. Philippe Latombe, rapporteur. En ce sens, le gouvernement a débloqué des fonds dédiés aux collectivités territoriales en matière de cybersécurité. Sont-ils suffisants ?

M. Michel Van Den Berghe. Il s'agit d'un premier pas très important. La création d'antennes régionales permettant de mettre en place des systèmes sécurisant les collectivités locales, les hôpitaux, etc., est un excellent premier pas. Le plan de relance et d'accélération cyber, avec le milliard d'euros consacré au développement des outils cyber est extrêmement important. La prise de conscience est là : il faut maintenant accompagner l'ensemble des collectivités territoriales et protéger les plus faibles. On le voit : pour attaquer une grande entreprise, le pirate vise fréquemment son sous-traitant, qui est plus vulnérable, et peut faire entrer le virus dans le système d'information de la grande entreprise. Nous devons nous mobiliser pour proposer des solutions aux très petites entreprises (TPE), qui n'ont parfois même pas de DSI. Si nous ne les aidons pas, elles constitueront des portes d'entrée vers les administrations ou les grandes entreprises.

M. Philippe Latombe, rapporteur. Qui serait selon vous le bon prescripteur ? Serait-ce Bpifrance ? Je ne parle pas des grands groupes, qui peuvent par ruissellement demander à leurs sous-traitants de se sécuriser, ce qu'ils ont commencé à faire, mais pour tous les acteurs qui ne se trouvent pas dans cette situation, quel serait le bon prescripteur de la réflexion cyber, au-delà du Campus Cyber, qui constitue en soi un centre de ressources ? Le prescripteur devrait-il être Bpifrance, lorsqu'elle investit pour numériser ou modifier le système d'information, l'expert-comptable, l'un des interlocuteurs assez naturels des dirigeants de PME, TPE ou même ETI ? Quel est selon vous le bon niveau ?

M. Michel Van Den Berghe. C'est véritablement la question que nous nous sommes posée. Selon nous, trois acteurs atteignent un maximum de ces entreprises. Le premier est le banquier, car toutes les entreprises ont un compte en banque : les banquiers pourraient proposer une solution la plus simple possible à télécharger sur un kiosque pour protéger les PC. La Poste est également un interlocuteur évident : tout le monde reçoit du courrier, et il existe une relation de confiance avec le facteur. Enfin, les opérateurs réseau qui apportent de la connectivité pourraient également proposer des solutions simples à installer, pour fournir un minimum de cybersécurité.

Sans faire de publicité à Orange Cyberdéfense, je suis précisément en train de travailler sur le sujet, en essayant d'inciter Orange France à mettre en place une solution que nous sommes en train de construire avec les sociétés françaises Tehtris et Vade Secure. Il s'agit d'une solution de type *endpoint detection and response (EDR)*, qui remplace l'antivirus et isole un poste de travail du réseau lorsqu'elle y détecte des comportements malveillants, afin d'éviter la contamination de l'ensemble de l'entreprise. Vade Secure apporte une solution d'*antifishing*, qui détecte les pièces malveillantes dans les mails et les met de côté, permettant d'éviter que les utilisateurs cliquent dessus et infectent leur poste de travail. Nous essayons également de faire en sorte que la solution soit très peu chère : la campagne que nous mènerons sera intitulée « Votre cybersécurité pour le prix d'un café ». Nous souhaitons que cette solution coûte moins de 40 centimes d'euro par jour.

J'incite Orange France à proposer cette application avec les *box* pour professionnels. Nous pourrions le faire également avec les banquiers, avec les assureurs, qui pourraient diminuer la police d'assurance moyennant cette amélioration de la sécurité.

Chez Orange, le marché des professionnels et des PME, constitué des entreprises de moins de cinquante salariés, regroupe cinq millions de clients. En Europe, ces sociétés représentent 99 % des entreprises. Il existe donc un intérêt y compris financier à proposer ce type de solutions. Je me bats chez Orange pour qu'une solution soit proposée sur un kiosque, à destination des entreprises d'un à cinq salariés, afin qu'elles disposent d'un dispositif d'antivirus, de détection comportementale et d'*antifishing* pour trente ou quarante centimes d'euro par poste de travail et par jour. Les clients adhéreraient assez facilement à un tel outil.

M. Philippe Latombe, rapporteur. Nous avons parlé des clients. Si nous parlons de l'offre, vous avez évoqué dans votre propos liminaire le morcellement des acteurs, qui travaillent sur des segments parfois compatibles ou complémentaires les uns des autres. Comment structurer l'ensemble ? L'objet du Campus est-il précisément d'agréger les solutions, pour pouvoir aborder les marchés de façon commune, ou s'agit-il simplement de faire émerger les entreprises en dehors de cette logique ? À terme, le marché peut-il rester aussi hétérogène ?

M. Michel Van Den Berghe. Vous pointez bien la faiblesse du marché de la cybersécurité. Les quatre grandes entreprises industrielles du secteur représentent 80 % du marché, ce qui n'est pas idéal. Orange Cyberdéfense cherche à faire de la croissance externe, mais ne trouve pas d'entreprises à acheter, y compris en Europe, hormis des sociétés qui réalisent 20 à 25 millions d'euros de chiffre d'affaires. Nous trouvons peu de cibles potentiellement accessibles.

Il faut parvenir à structurer ce marché de la cybersécurité, l'amener dans les régions, car la proximité est extrêmement importante. L'objectif du Campus Cyber est précisément d'aider à faire connaître ces PME, qui apportent de la cybersécurité dans les régions. Quelques entreprises sont assez fortes dans leurs différentes régions – Advens à Lille, Tehtris à Bordeaux, etc. Nous devons créer un maillage, et faire en sorte que les gens se parlent pour élever le niveau global de cybersécurité. Notre premier objectif est de créer une base de marqueurs, pour que les personnes qui font de la détection puissent s'y connecter. Chacun doit oublier un peu la concurrence pour que le même niveau de détection soit possible partout dans le pays.

Nos *start-up* doivent également pouvoir évoluer et s'internationaliser sans nécessairement aller chercher des fonds outre-Atlantique. Il ne faut plus que les entreprises françaises qui commencent à bien fonctionner sur le territoire national soient obligées de créer un siège social à San Francisco pour pouvoir rayonner aux États-Unis. Il est possible de procéder autrement, mais nous devons nous en donner les moyens. Nous devons conserver des entreprises françaises capables de s'adresser à des clients internationaux sans basculer leur siège social aux États-Unis.

M. Philippe Latombe, rapporteur. On nous dit très régulièrement, lors des auditions, que l'amorçage est une bonne chose, mais qu'il importe plus d'avoir des clients que des subventions. L'État joue-t-il aujourd'hui correctement son rôle de client ? Peut-il mieux faire, et le cas échéant comment ? Les grandes entreprises, qui ne suivent pas des procédures de marchés publics, mais ont de grands besoins, font-elles, de leur côté, suffisamment d'efforts pour recourir à des *start-up* ?

Par ailleurs, vous indiquez ne pas trouver de cibles à acheter. Or, on nous explique depuis le début des auditions que personne ne veut les acheter en France, et qu'il est obligatoire de se vendre à l'étranger. Comment résolvons-nous ce paradoxe ?

M. Michel Van Den Berghe. La question est très pertinente. En France, nous sommes très doués pour incuber. De très nombreuses sociétés sont placées dans des couveuses, soutenues par des banques, bénéficient de bureaux, de moyens de se développer, etc. La phase la plus compliquée est celle de l'industrialisation et du décrochage de grands clients permettant à ces entreprises d'avoir une autonomie de financement assez importante.

J'ai été entrepreneur. Lorsque vous créez votre solution, même si elle est extrêmement pertinente, et que vous vous retrouvez face aux acheteurs des grandes sociétés françaises, ils constatent que les techniciens ont validé la solution, mais vous demandent vos trois derniers bilans, demandent la garantie que vous êtes capable de payer un million d'euros de pénalités si la solution détériore le système d'information de l'entreprise, etc. Toutes ces contraintes liées aux politiques d'achat expliquent qu'il n'est pas possible de servir ces grandes sociétés.

Le combat que j'ai mené avec Orange Cyberdéfense vise à répondre à cette difficulté. Lorsqu'une société est pertinente d'un point de vue technologique, nous la plaçons très rapidement à notre catalogue, pour rassurer les clients potentiels. Orange Cyberdéfense, société qui réalise 800 millions d'euros de chiffre d'affaires, prend en charge la contractualisation, couvre les risques de pénalité, etc. Cela accélère véritablement la possibilité pour des petites entreprises d'atteindre de très grands comptes.

Le dernier exemple en date est la société Alcide, créée à Annecy.

M. Philippe Latombe, rapporteur. Nous en avons entendu parler.

M. Michel Van Den Berghe. Orange Cyberdéfense a mis Alcide à son catalogue et a incité ses propres clients à acheter ses solutions, en prenant en charge les problématiques de référencement et d'achat. *In fine*, Alcide a été racheté par une société américaine, pour un montant de 100 millions d'euros – ce qui est heureux pour les fondateurs, mais casse la concurrence. Personne en France ne peut investir 100 millions d'euros pour acheter Alcide. Cette valorisation est complètement délirante. La valorisation des cibles du marché de la cybersécurité est pour nous de l'ordre de 20 à 25 % de l'EBITDA. Je ne peux pas demander au conseil d'administration de valider l'acquisition d'une entreprise pour un montant de vingt à vingt-cinq fois son EBITDA, quand Orange Cyberdéfense est pour sa part valorisée deux à trois fois son EBITDA. Le marché est survalorisé. Aucune entreprise française ne peut débourser 100 millions d'euros pour acheter Alcide, qui réalise 8 millions d'euros de chiffre d'affaires.

M. Philippe Latombe, rapporteur. Pour quelle raison l'acquéreur est-il prêt à payer cette somme ? Il existe bien une raison économique chez l'acheteur. Nous ne parlons pas de philanthropie, ou de l'achat du *Salvator Mundi*. Alcide n'est pas un trophée que l'on affiche dans une vitrine.

M. Michel Van Den Berghe. Il existe certainement un intérêt. Je suis plus un technicien qu'un financier, mais c'est la rareté des opportunités qui explique des valorisations aussi délirantes. Alcide propose une technologie excellente, qui gère la sécurisation du référencement des utilisateurs. Son seul concurrent est Microsoft. Cela peut effectivement être intéressant pour une entreprise américaine, qui, vu sa portée, pourra peut-être dégager très rapidement de la rentabilité. Lorsque vous achetez une entreprise vingt-cinq fois la valeur de son EBITDA, cela signifie cependant qu'il faut vingt-cinq ans pour rentabiliser l'investissement. Il faut donc être certain que les synergies d'acquisition permettront de

diviser le coût par deux. Dans notre métier, les valorisations sont de manière générale un peu délirantes.

M. Philippe Latombe, rapporteur. Les grandes entreprises achètent relativement cher ces sociétés, c'est-à-dire une vingtaine de fois l'EBITDA plutôt que deux à trois fois l'EBITDA. Est-ce parce qu'elles achètent quelque chose qu'elles ne maîtrisent pas, ou qui est en concurrence potentielle avec ce qu'elles sont en train de développer et qu'elles veulent donc détruire ? Que faudrait-il faire en France pour préserver ces sociétés, ou pour procéder de même ? Ne disposons-nous pas de suffisamment de grandes entreprises capables de réaliser ces acquisitions ?

M. Michel Van Den Berghe. C'est un peu ce que nous essayons de construire : nous voulons créer des industriels européens capables de « challenger » les grands acteurs américains. Si nous étions déjà capables d'accompagner toutes les entreprises européennes dans leur mondialisation, on offrirait un terrain de jeu extrêmement important. Nous devons créer des acteurs européens capables de « challenger » ces grands acteurs américains, et de peser face aux GAFA. Palo Alto, etc., qui sont visionnaires dans la transformation numérique et achètent des *start-up* qui ont déjà développé des solutions, pour ne pas avoir à le faire eux-mêmes. Même s'ils ont commencé à travailler dans le domaine, mais qu'une *start-up* est allée plus vite, ils l'achètent, la mettent à leur catalogue et sont en avance sur le marché. Nous devons créer ces acteurs français, européens, capables de rivaliser avec les grands acteurs américains pour acquérir les entreprises innovantes et positionner leurs offres sur le marché mondial.

Nous commençons à le faire. Nous l'avons par exemple aux États-Unis et; c'est la première fois qu'un acteur européen pénètre le marché américain, peut-être grâce à l'image plus transparente des entreprises européennes en matière de données. Nous devons créer de grands acteurs européens, avec la même expertise que les grands acteurs américains, pour créer de la valeur. Toutes les grandes entreprises européennes doivent être accompagnées dans leur conquête du marché mondial. Nous avons, par exemple, créé un *data center* en Chine pour accompagner un géant du luxe souhaitant pénétrer le marché chinois. Nous avons fait de même pour un fabricant de meubles suédois, qui voulait attaquer le même marché, car les données du personnel et des clients doivent rester sur le territoire chinois. Nous sommes capables de le faire, mais nous devons accélérer pour atteindre une taille nous permettant de lutter contre les GAFA et un jour peut-être investir les mêmes montants pour éviter que nos pépites françaises soient achetées par des entreprises américaines.

M. Philippe Latombe, rapporteur. Le Campus Cyber permettra-t-il aux *start-up* françaises, mais également à l'ensemble de l'écosystème, de « chasser en meute » ?

M. Michel Van Den Berghe. C'est exactement ce que nous voulons faire. Nous voulons nous rassembler pour pouvoir « chasser en meute », et créer la connexion. La France réussit très bien la phase d'incubation. Nous devons désormais créer des liens pour que les *start-up* devenues des PME soient très rapidement mises au catalogue des grands industriels, et que ces derniers les aident à se développer et à proposer leurs solutions dans l'ensemble du territoire. Lorsque Thales ou Atos mettent à leur catalogue la technologie d'une PME française, celle-ci se développe beaucoup plus vite, car elle peut atteindre de grands comptes. C'est la phase d'industrialisation qui est compliquée pour les PME.

J'ai revendu Atheos à Orange, parce que les grands comptes estimaient que l'entreprise commençait à prendre trop de poids à l'intérieur de grands industriels français, et

que sa puissance financière les dérangeait. J'ai donc décidé de m'adosser à un grand industriel pour continuer à monter en expertise et en puissance au sein de ces grands comptes. Il s'agit d'une belle réussite : le chiffre d'affaires d'Atheos était de 30 millions d'euros en 2014, en y ajoutant les activités d'Orange, le périmètre était de l'ordre de 80 millions d'euros. Orange Cyberdéfense réalise en 2020 près de 800 millions d'euros de chiffre d'affaires.

Lorsque nous créons un acteur français capable d'apporter la même expertise que les sociétés américaines, les clients suivent. Tout le CAC 40 est aujourd'hui client d'Orange Cyberdéfense, et a choisi, à expertise égale, l'acteur français plutôt que son concurrent américain.

M. Philippe Latombe, rapporteur. J'en viens à ma dernière question. Comment gérer l'extraterritorialité américaine ? Devons-nous jouer avec, créer nos propres règles en Europe ? Comment voyez-vous les choses ?

M. Michel Van Den Berghe. Nous devons créer nos propres règles en Europe.

Lorsque nous avons créé le Campus Cyber, de nombreux acteurs américains et chinois m'ont demandé d'y participer, de prendre des actions, etc. Je leur ai demandé de nous laisser nous organiser avec des acteurs français, peut-être des acteurs européens, en remarquant qu'un Campus Cyber aux États-Unis n'accepterait pas Orange Cyberdéfense dans sa gouvernance sans rien lui demander en contrepartie. L'Europe doit s'organiser pour créer une régulation du marché de la cybersécurité. Cette « meute » française doit être organisée au niveau de l'Europe, pour que nous puissions faire émerger ces grands acteurs de la cybersécurité et pouvoir attirer les grandes sociétés internationales.

M. Philippe Latombe, rapporteur. Quels points n'aurions-nous pas abordés, que vous voudriez évoquer ?

M. Michel Van Den Berghe. Il ne s'agit pas de votre première audition, et vous avez à mon avis bien cerné les questions. Les sujets sur lesquels nous devons travailler ensemble sont la sensibilisation de l'écosystème industriel à la problématique de la cybersécurité et le changement d'image de la cybersécurité, pour créer des vocations, expliquer que la cybersécurité n'est pas anxiogène, que ce métier a beaucoup de sens. Nous avons besoin de spécialistes de la législation, de la communication, etc., et de supprimer l'image que nous voyons trop souvent dans les reportages du geek avec une capuche, que je ne supporte plus.

M. Philippe Latombe, rapporteur. Nous ne vous en présenterons pas.

M. Michel Van Den Berghe. Nous devons changer cette image.

La perception du sujet par les dirigeants doit aussi évoluer. Au départ, lorsque nous voulions intervenir dans les comités exécutifs, on nous expliquait que le sujet était trop anxiogène et technique. Les mentalités commencent à changer. Il faut expliquer que la cybersécurité fait partie de la transformation numérique et qu'en la prenant en compte le plus rapidement possible, par le *secure by design*, on s'évite bien des problèmes.

La séance est levée à 11 heures 05.

Membres présents ou excusés

Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du mardi 13 avril à dix heures

Présents. – M. Philippe Latombe, Jean-Luc Warsmann