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
30 mars 2021
Séance de 11 heures

Compte rendu n° 50

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. David Ofer, président de la Fédération française de la Cybersécurité

La séance est ouverte à 11 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons M. David Ofer, président de la Fédération française de la Cybersécurité, association ayant vocation à rassembler les professionnels de la cybersécurité, avec l'objectif de contribuer à la structuration de cette filière. Organisés en plusieurs collèges thématiques, vous assurez la promotion de la formation aux compétences cyber et innovation. Nous souhaiterions aborder avec vous les questions tenant à la certification et à la labellisation des solutions de cybersécurité.

M. Philippe Latombe, rapporteur. Comment appréhendez-vous la notion de souveraineté numérique ? De quelle façon les politiques menées peuvent ou doivent-elles évoluer pour mieux l'intégrer le cas échéant ?

Ensuite, je souhaiterais que nous puissions échanger à propos de l'écosystème des entreprises françaises de la cybersécurité. Comment ces entreprises se portent-elles dans le contexte actuel de crise sanitaire durable ? Quels sont leurs besoins et leurs attentes vis-à-vis des pouvoirs publics ? Quelles sont leurs propositions pour participer à la construction d'une forme de souveraineté numérique ? Comment faire en sorte que l'écosystème cyber français continue de se développer et de se renforcer ? Ce thème nous permettra d'aborder les annonces récentes du Président de la République et l'actualité européenne marquée par la révision de la directive *NIS (Directive on security of network and information systems)* et par la présentation d'une stratégie cyber par la Commission européenne, à la fin de l'année dernière.

Enfin, s'agissant de la diffusion d'une culture cyber au sein de la société, quel regard portez-vous sur le niveau de sensibilisation des entreprises, des administrations publiques, des collectivités territoriales et des citoyens ? Je souhaiterais aussi que nous évoquions la formation aux compétences cyber alors qu'un campus cyber est en cours de développement, avec l'appui, notamment, de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Comment la France se positionne-t-elle par rapport aux autres pays ? Existe-t-il des segments sur lesquels nous devrions compléter notre offre de formation pour combler d'éventuelles lacunes.

M. David Ofer, président de la Fédération française de la Cybersécurité. La Fédération française de la Cybersécurité a pour objet de rassembler toutes les organisations, les associations professionnelles, les entreprises, les personnes et, plus largement, tous les acteurs directs ou indirects liés à la cybersécurité.

Comme vous le savez, il existe un grand nombre d'associations et d'initiatives qui parlent aujourd'hui de manière dispersée. Au regard de l'actualité et de l'évolution sociétale, il est important de coordonner les actions sur la cybersécurité, en consolidant une filière qui est marquée et représentée, beaucoup trop souvent, par la dimension technique du sujet. Notre ambition est bien de coordonner l'ensemble de ces actions.

La cybersécurité est un élément incontournable de la vie du citoyen et des entreprises. Elle doit d'inscrire dans la lignée de la responsabilité sociétale et environnementale des

entreprises, car l'impact d'une cyberattaque pénalise gravement le tissu économique et la souveraineté. La notion de souveraineté est liée à l'indépendance, celle de nos citoyens, de nos entreprises et plus largement de notre pays.

Ce qui devient aujourd'hui un véritable défi sur les sujets de cybersécurité ne peut se réaliser pleinement qu'en fédérant les acteurs existants, qui peuvent apporter, chacun dans son périmètre, des savoir-faire qui feront avancer cette souveraineté et la replaceront à l'ordre du jour. Si nous souhaitons aller dans cette direction, tous ensemble, il faut adapter notre vision et créer un cercle vertueux, où l'État jouera son rôle pour insuffler une politique, les agences techniques apporteront des garanties, les grands groupes pourront utiliser les moyens financiers et les PME créer de la valeur et une proximité avec le terrain. L'objectif doit être la protection du citoyen et du tissu économique et, par incidence, la protection des institutions.

La Fédération française de la Cybersécurité souhaite consolider cette filière en portant des messages représentatifs sur les problématiques rencontrées, mais aussi mener des actions de terrain pour remplir les objectifs que j'évoquais précédemment.

Parmi les actions que nous avons lancées pour le maillage territorial que nous souhaitons promouvoir, je citerai notre plan de création de 20 000 emplois sur la base d'un nouveau métier dédié aux jeunes non diplômés ou à des personnes souhaitant se reconvertir professionnellement. Ce nouveau métier d'assistant cyber a pour vocation de créer une proximité de terrain avec les utilisateurs du numérique, en informant et en complétant notamment le rôle des ingénieurs et des spécialistes techniques qui ont déjà fort à faire. Les premières formations vont débuter cet été.

Autre action concrète, la mise en place d'un soutien direct aux PME par la réalisation d'un diagnostic de cybersécurité gratuit qui permettra leur prise de conscience et les aidera, lorsqu'elles auront subi une cyberattaque, en les dispensant de payer la franchise d'assurance qu'elles auraient souscrite. Nous estimons le coût de cette opération de diagnostic à 20 millions d'euros environ, montant que nous espérons collecter auprès de l'État et des collectivités territoriales.

La Fédération française de la Cybersécurité mène des actions concrètes, de proximité, pour encourager au maximum la protection du tissu économique et la souveraineté française avec un esprit altruiste et citoyen.

Je peux poursuivre si vous le souhaitez avec un état des lieux et quelques chiffres qui permettraient d'avoir un peu de visibilité sur ce qui se passe aujourd'hui en France et à l'étranger.

M. Philippe Latombe, rapporteur. Très bien.

M. David Ofer. Les chiffres sur la menace cyber sont sous-estimés, et ce pour plusieurs raisons. D'abord, les chiffres sont basés sur les déclarations des attaques, sur les plaintes des victimes et sur les interventions de l'ANSSI et des forces de l'ordre. Or toutes les attaques ne sont pas déclarées. Un grand nombre de statistiques proviennent d'entités non indépendantes de type cabinets de conseils ou éditeurs.

L'ANSSI a réalisé 192 interventions en 2020, soit une augmentation de 200 % par rapport à 2019. Cybermalveillance de son côté a recensé 837 entreprises et 159 collectivités attaquées. Par ailleurs, les compilations de chiffres que nous avons de notre côté montrent que

neuf organisations sur dix sont victimes de cyberattaques. Il faut noter qu'une cyberattaque n'est pas forcément une paralysie du système d'information. Selon une étude d'un spécialiste de la cybersécurité, 91 % des organisations françaises ont été la cible de cyberattaques cette année et 60 % ont subi plusieurs actes malveillants. 75 % et plus des attaques sont faites par des *ransomwares* (rançongiciels) en France comme dans le reste du monde.

Dans le classement mondial du nombre de détections arrivent en premier les États-Unis, le Japon, puis l'Inde. L'Espagne est en 8ème position de ce classement mondial, l'Allemagne en 10ème, l'Italie en 11ème et la France en 16ème. Les pays européens les plus touchés par les rançongiciels sont l'Allemagne en tête, suivie de la France, de l'Italie et du Royaume-Uni.

Une unité du FBI aux États-Unis, l'*IC3* (*Internet Crime Complaint Center*) recense l'intégralité des plaintes liées au cybercrime. L'*IC3* a annoncé une moyenne de 791 790 plaintes pour 2020 et 4,2 milliards de dollars de pertes pour les États-Unis. Nous n'avons pas ce genre de chiffres en France, parce que nous ne les recensons pas de la même manière.

En nombre de plaintes déposées, le Royaume-Uni arrive en première position avec 216 000 plaintes, suivi par le Canada (5 300), l'Inde (2 930). La France est septième dans ce classement avec 1 640 plaintes déposées par des victimes en 2020. Il existe une différence colossale entre le nombre d'attaques non référencées et le nombre de plaintes déposées.

Enfin, selon un éditeur d'antivirus, la cybercriminalité coûterait environ 1 000 milliards de dollars à l'économie mondiale.

M. Philippe Latombe, rapporteur. En quoi la cybersécurité est-elle une composante essentielle de la souveraineté numérique ? A-t-on aujourd'hui les moyens de pouvoir être souverain dans ce domaine de la cybersécurité ?

M. David Ofer. Les chiffres d'affaires des entreprises françaises qui sont annoncés en cybersécurité incluent beaucoup d'assistance technique, le chiffrement, les matériels télécoms, l'identification des personnes. Les logiciels utilisés aujourd'hui sont américains pour la plupart, notamment les systèmes d'exploitation, la bureautique, les bases de données, le *cloud* et les usages grand public. Les éditeurs étrangers commercialisent auprès de nos entreprises des produits qui comportent des failles de cybersécurité. Ainsi, Microsoft corrige en moyenne 100 vulnérabilités par mois ces derniers temps.

Est-ce normal ? Accepterait-on de rouler avec une voiture dont les freins sont défaillants ? Je ne sais pas. Il nous manque en France des champions en cybersécurité dans les secteurs du futur, en associant notamment l'Intelligence artificielle.

Dans le domaine des produits de cybersécurité, nous avons un tissu économique qui est fort, mais nous sommes démunis ce qui concerne le socle technologique qui traite du numérique. Nous n'avons pas de système d'exploitation français. Nous n'avons ni système de bureautique ni système de base de données français. Le *cloud* est un grand débat. Aujourd'hui, nous utilisons pour cette visioconférence un logiciel américain alors qu'il existe d'excellents logiciels français de visioconférence.

La problématique de la souveraineté passe aussi par le soutien des entreprises françaises, par un certain nombre de mesures à mettre en place. Le plan cyber que le Président de la République a annoncé est, certes, une excellente avancée, mais il est insuffisant.

Pour donner des chiffres, Israël a levé l'an dernier 2,6 milliards de dollars pour la cybersécurité. Notre plan représente un milliard d'euros, dont un peu plus d'une moitié financée par l'État et le reste par le privé. Au regard de notre population qui est dix fois plus importante que celle d'Israël, il nous aurait fallu *a minima* 26 milliards de dollars.

En Intelligence artificielle et en cybersécurité, nous sommes très loin derrière les investissements astronomiques chinois.

M. Philippe Latombe, rapporteur. Avez-vous des propositions à nous soumettre ?

M. David Ofer. Tout à fait. Il faudrait créer un *small business act*, c'est-à-dire inciter très fortement les mairies, les collectivités territoriales, les institutions publiques et parapubliques à acheter des logiciels et produits français en allant au-delà de la simple recommandation. Je peux vous donner des exemples très précis. L'aéroport de Nice choisit un produit américain pour sa cyberdéfense, Agirc-Arrco choisit des produits étrangers, la métropole de Nantes choisit des produits américains alors qu'en France, nous avons des produits de premier ordre qui sont aussi bons que les produits étrangers, notamment américains.

Souhaitons-nous une souveraineté, c'est-à-dire une indépendance ? Souhaitons-nous pousser notre industrie et favoriser notre tissu économique ou laisser la porte ouverte à des pays étrangers pour assurer notre cybersécurité ?

M. Philippe Latombe, rapporteur. Dans les exemples que vous avez cités, qu'est-ce qui a emporté le choix ? Le code des marchés publics ? Les acheteurs qui ne sont pas curieux et qui ont pris ce qu'ils avaient sur étagère ? Est-ce une forme d'entrisme des Américains ?

M. David Ofer. Le code des marchés publics oblige quasiment à mettre en place une grille tarifaire. Quand une société qui a des moyens colossaux accorde une remise de 90 % sur le prix de ses produits pour pénétrer un marché, une PME française n'a pas les moyens de s'aligner.

Il existe tout un écosystème américain. Les États-Unis ont mis en place depuis des années une politique visant à faire rayonner leur économie avec le *Small Business Act*. Il faut absolument créer un *small business act* à la française. Il faut absolument que l'on puisse, dès qu'une PME émerge dans la cybersécurité, lui proposer des marchés avec les services de l'État, des collectivités territoriales sans que cela soit un frein au développement.

M. Philippe Latombe, rapporteur. N'est-ce pas le rôle des intégrateurs d'être dans le conseil et dans le choix de solutions souveraines ?

M. David Ofer. Je ne rejoins pas tout à fait cette vision. Aujourd'hui, les grands groupes français intégrateurs de solutions de cybersécurité commercialisent des produits américains alors qu'il existe des équivalents français. Pour quelle raison ? Nous avons vécu la même situation avec les PC et la téléphonie mobile. On n'a pas aidé nos entreprises françaises parce que ces intégrateurs vont chercher la facilité et uniquement la valeur ajoutée sur le prix de vente. On n'a pas une vision de défense du tissu économique. On a des articles très intéressants sur le ruissellement économique. Quand vous achetez un logiciel français, vous

créez de l'emploi en France, vous créez de la valeur ajoutée pour le tissu économique, vous créez de la proximité avec nos institutions, vous créez des capacités pour le tissu économique français à aller rayonner au-delà des frontières. Toute cette création de richesse, vous ne l'avez pas quand vous achetez un logiciel américain.

M. Philippe Latombe, rapporteur. L'État, les administrations publiques, les collectivités territoriales, les entreprises et les citoyens sont-ils suffisamment acculturés à la cybersécurité ?

M. David Ofer. Toutes les collectivités territoriales que je rencontre sont sensibilisées au risque cyber.

Il faut se poser la question de ce qu'est le risque cyber. Est-ce uniquement la paralysie par une attaque ou est-ce également la possibilité d'avoir accès à nos données ? Là se pose une question de politique : est-on prêt à laisser l'accès à nos données à tout le monde ? Ou veut-on avoir une politique souveraine sur la protection de nos données ?

Les collectivités territoriales sont parfaitement conscientes des enjeux de cybersécurité. Les directeurs des systèmes d'information (DSI) et les responsables de la sécurité informatique que je rencontre sont les premiers à essayer d'acheter des outils de cybersécurité. Ils font appel à l'ANSSI qui joue un rôle très important. Ils essayent de sensibiliser leurs utilisateurs, mais aujourd'hui, les collectivités territoriales n'ont pas toujours des moyens financiers et humains suffisants. Aujourd'hui, nous souffrons d'une pénurie forte d'ingénieurs : il manque trois à quatre millions d'ingénieurs en cybersécurité. On ne pourra pas former en France plusieurs centaines de milliers d'ingénieurs en deux ans. Il faut cinq, six, sept ans.

Cette problématique des moyens est un véritable sujet. Pour cette raison, la Fédération française de la Cybersécurité a prévu le nouveau métier d'assistant cyber, qui sera le relais entre la dimension technique de la cybersécurité et l'utilisateur, notamment dans les collectivités territoriales.

Je vais prendre un exemple simple. La plupart des agents dans les mairies ne savent pas changer leur mot de passe. Il faut un accompagnement pour ces personnels pour garantir la cybersécurité.

Oui, il y a une prise de conscience réelle dans les collectivités territoriales. Cela dit, les élus ne prennent pas toujours des décisions adéquates parce qu'ils manquent de connaissance en matière de cybersécurité. Ils ne voient que le risque de paralysie, et pas la problématique de l'exfiltration de données. La stratégie des *smart cities* peut être mise en péril à partir du moment où vous donnez un accès non autorisé à vos données à un tiers.

M. Philippe Latombe, rapporteur. Dans le plan de relance, le plan cyber est aussi dirigé vers les collectivités territoriales. Vous dites qu'elles manquent davantage de moyens humains que de moyens financiers.

M. David Ofer. Les deux. Vous avez de grandes collectivités territoriales qui ont des moyens, mais les petites mairies ont des ressources limitées. Dans une mairie que je ne citerai pas, ma rencontre avec les responsables de l'informatique a été fort intéressante. Par décision des élus, ils disposaient d'un budget de 5 000 euros pour la cybersécurité, contre 1,5 million d'euros pour la vidéosurveillance.

Au-delà de l'argent, il faut qu'il y ait cette volonté et cette prise de conscience que la cybersécurité est un enjeu de protection du citoyen. Nous l'avons vu avec la paralysie des hôpitaux.

M. Philippe Latombe, rapporteur. Ne faudrait-il pas parler davantage des cyberattaques et de leurs conséquences ? Quand les hôpitaux ont été attaqués, on s'est rendu compte qu'ils n'avaient pas de plan de continuité d'activité. Suite à l'attaque de la ville d'Angers, une partie entière de l'activité est bloquée. Ils n'arrivent toujours pas à accéder aux données des horodateurs.

M. David Ofer. Communiquer sera toujours bénéfique, mais ne résoudra pas tout. La communication ne vous protégera pas des failles de sécurité que vous pouvez avoir dans les logiciels et dans les systèmes d'exploitation que vous achetez. Le seul moyen, c'est d'avoir une vision véritablement sociétale de la cybersécurité et peut-être d'avoir une approche à l'américaine, c'est-à-dire de quantifier très précisément le coût des cyberattaques. Aujourd'hui, des statistiques démontrent que plus de la moitié des entreprises qui ont vécu une cyberattaque sont absolument incapables de donner un chiffre précis du coût de celle-ci. 50 % des PME qui ont vécu une cyberattaque paralysante disparaissent dans les six mois qui suivent. Les grands groupes qui subissent des cyberattaques perdent, s'ils ne font rien, 20 % de leur valorisation, six à huit mois après. Ce sont des sommes colossales ! On ne pourra pas compenser ces problématiques uniquement avec de la communication, il faut des actions, il faut soutenir la filière de la cybersécurité, de manière à essayer de promouvoir ce tissu économique et de défendre nos institutions, nos entreprises et le citoyen.

M. Philippe Latombe, rapporteur. Il est communément admis que la France a un très haut niveau d'expertise en cybersécurité, que l'ANSSI est moteur dans la cybersécurité, que nous avons un écosystème de cybersécurité très à la pointe du progrès, qui suscite même des envies. Est-ce vrai ? Avons-nous des pépites qu'il faut absolument protéger ? À l'inverse, avons-nous des lacunes ?

M. David Ofer. Oui, nous avons un excellent écosystème français, parce que nous avons beaucoup d'entreprises qui développent de la technologie en cybersécurité avec des produits très innovants. L'ANSSI joue un rôle important pour les grandes entreprises.

Cela dit, quand on regarde la Suisse et la Grande-Bretagne, quand on regarde comment sont équipées les entreprises en termes de cybersécurité, les logiciels américains et israéliens dominent le marché.

L'écosystème français est bon et performant. Nous avons des logiciels et des ingénieurs de premier plan. Le vrai sujet est le suivant : comment promouvoir ces entreprises au-delà de nos frontières ? Je reviens à ma proposition de *small business act* à la française. Il faut aider nos entreprises à obtenir des marchés, il faut être capable d'investir massivement dans ces entreprises.

En 2016, un rapport américano-anglais présentait deux pépites françaises de la cybersécurité comme des licornes en devenir : Pradeo et ITrust. Ces deux entreprises ont levé respectivement un et deux millions d'euros, alors que deux entreprises américaines, Palantir et Tenable ont levé des centaines de millions et rayonnent sur le marché de la cybersécurité au niveau mondial.

Si l'on veut favoriser nos entreprises, il faut investir et aider les entreprises à accéder à des marchés, ce qui passe par la commande publique, par la génération de chiffre d'affaires et par un rôle d'accompagnement des autorités. L'ANSSI délivre des certifications qui sont utiles pour les grands groupes, mais elle devrait avoir un rôle de conseil et d'accompagnement pour les entreprises à l'export.

Il existe un grand nombre de certifications, mais aujourd'hui, la problématique est l'investissement dans les pépites et l'écosystème. Le plan d'un milliard est nécessaire, mais il faut aller au-delà. Pour faire une licorne, il faut investir dans une entreprise entre vingt et cinquante millions d'euros. Je ne connais pas un fonds français qui est prêt à investir un tel montant sur une entreprise qui ne réalise pas de chiffre d'affaires. Toute la problématique se situe à ce niveau. Aux États-Unis, en Israël et dans quelques autres pays, vous avez des entreprises qui, avec quelques centaines de milliers d'euros de chiffre d'affaires, lèvent des centaines de millions et deviennent de véritables champions.

En France, nous avons laissé filer des pépites. Je veux vous donner l'exemple de Sentryo, qui a été créée par un entrepreneur français qui a développé une solution pour vérifier l'*IoT (Internet of the Things)*. Il a fait le tour des investisseurs français, qui ont regardé son dossier avec dédain. À cours de solutions, cet entrepreneur courageux a été obligé de passer sous drapeau américain. Malheureusement, les décideurs français regardent les dossiers d'investissement avec un œil de banquier, et non avec une prospective de souveraineté dans l'intérêt du tissu économique national.

M. Philippe Latombe, rapporteur. Voulez-vous dire qu'aujourd'hui, les entreprises de la cybersécurité sont trop petites et devraient se regrouper afin de pouvoir atteindre une taille critique qui leur permet d'avoir accès à des marchés plus gros et à des financements plus importants ?

M. David Ofer. Non, il faut qu'il y ait une floraison d'entreprises, parce que plus vous aurez d'entreprises qui vont émerger, plus vous aurez la chance d'avoir, au travers de l'une d'entre elles, des champions qui pourront créer de l'emploi, promouvoir notre économie et défendre notre souveraineté. C'est ce que nous n'avons pas aujourd'hui par manque de moyens.

M. Philippe Latombe, rapporteur. La floraison ne rend-elle pas plus difficile l'intégration de ces solutions dans le système d'information des clients ? Ne génère-t-elle pas un problème d'interopérabilité ?

M. David Ofer. La multiplicité des acteurs de la cybersécurité est liée à la multiplicité des outils informatiques. Un système d'exploitation ne se sécurise pas de la même manière qu'une base de données, qu'un réseau informatique, qu'un routeur, etc. Cette multiplicité de moyens demande une multiplicité d'outils de protection. Vous ne mettez pas un verrou sur une fenêtre, mais des barreaux.

M. Philippe Latombe, rapporteur. Si la cybersécurité est une conséquence d'une démarche d'ensemble (il faut que la cybersécurité soit présente sur l'ensemble de la chaîne numérique, de sa construction jusqu'à son utilisation), où faut-il investir aujourd'hui ? Où les entreprises de la cybersécurité doivent-elles être les plus proactives ?

M. David Ofer. Sur les systèmes d'information, la cybersécurité doit couvrir toute la chaîne. Vous ne sécurisez pas votre maison en laissant une fenêtre ouverte. C'est la raison

pour laquelle aujourd'hui, des méthodes de R&D pratiquent la *security by design*, c'est-à-dire intègrent les problématiques de cybersécurité dès le début. Aux États-Unis, c'est devenu un standard. En France aussi. Néanmoins, ce n'est pas suffisant. On voit que même des géants se font aujourd'hui cyberattaqués et que certaines solutions américaines que l'on croyait sécurisées ne le sont pas du tout.

Il faut déployer ce *security by design* à chaque niveau d'utilisation. La partie *IoT* arrive, avec les outils connectés. Là se pose une problématique de sécurisation de l'un des maillons que l'on ne maîtrise pas. Cela fait partie des défis qui sont lancés aujourd'hui aux acteurs de la cybersécurité.

M. Philippe Latombe, rapporteur. Quelles sont les trois actions qui devraient être mises en place, qu'elles soient financières ou législatives.

M. David Ofer. Il faut savoir de quoi l'on parle. Veut-on de la souveraineté avec une indépendance ou veut-on partager notre data avec nos alliés ?

Aujourd'hui, nous sommes dans une position de faiblesse extrême. Comment peut-on vouloir une souveraineté européenne à partir du moment où l'on utilise des produits et des technologies non européens ? Je peux prendre des exemples pour être concret. L'OSCE (Organisme de la Sécurité et de la Coordination européenne) a passé il y a deux ou trois ans un appel d'offres pour sa cybersécurité. Il n'utilise que des produits américains !

Quand on parle de souveraineté et d'indépendance, il faut faire des choix difficiles. Sommes-nous prêts à jeter nos téléphones portables ? À jeter les systèmes d'exploitation ? À changer toutes les habitudes des utilisateurs que certains appellent des consommateurs ? Aujourd'hui, si vous voulez acheter un téléphone mobile français, un système d'exploitation français ou un ordinateur français, vous aurez beaucoup de mal. Cette problématique a un impact sur la cybersécurité, car il est très difficile de sécuriser des systèmes que l'on ne maîtrise pas de bout en bout.

Microsoft présente des failles de cybersécurité qu'il corrige régulièrement. Finalement, vous vous retrouvez dans la situation dans laquelle vous achetez des produits américains et, parce qu'ils ne sont pas sécurisés, vous devez acheter des antivirus américains. Ce faisant, vous appauvrissez votre pays, vous enrichissez les États-Unis et en plus, vous subissez quand même des cyberattaques.

Si j'avais le pouvoir, je mettrais en place un fonds de soutien pour les entreprises qui se font cyberattaquer et une contribution obligatoire pour les entreprises étrangères qui commercialisent leurs logiciels en Europe. Il faut qu'à un moment, ces entreprises payent une contribution qui soit reversée aux entreprises victimes des cyberattaques qui sont permises par les logiciels qu'elles nous vendent. C'est un sujet sur lequel nous travaillons à la Fédération. Nous espérons que nous pourrons le mettre en place en France, avec votre aide. Si cette contribution est mise en place, elle obligera les fournisseurs étrangers à déployer des efforts conséquents pour améliorer la qualité des systèmes qu'ils nous vendent.

M. Philippe Latombe, rapporteur. Y a-t-il d'autres sujets que vous voulez évoquer ou des sujets sur lesquels vous voulez remettre l'accent ?

M. David Ofer. Non, je suis là pour répondre à vos questions. J'ai donné beaucoup d'informations et d'exemples très concrets. J'ai martelé qu'il fallait favoriser la commande de produits français dans la commande publique. J'espère que le message est passé.

M. Philippe Latombe, rapporteur. Le message est passé. Le sujet a été identifié dès le début des travaux de la mission d'information.

La séance est levée à 12 heures 10.

Membres présents ou excusés

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

Réunion du mardi 30 mars 2021 à 11 heures

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