ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Jeudi
17 décembre 2020
Séance de 11 heures

Compte rendu n° 19

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Denis Psomiades, président-directeur général de la Compagnie lyonnaise d'études et de services en systèmes électroniques (CLESSE)

La séance est ouverte à 11 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous auditionnons ce matin le président-directeur général de la Compagnie lyonnaise d'études et de services en systèmes électroniques (CLESSE), M. Denis Psomiades. La CLESSE est une petite et moyenne entreprise (PME) lyonnaise, spécialisée depuis trente-cinq ans dans le pilotage des moteurs électriques, qui a également développé une gamme d'ordinateurs nommés Business Computer, conçus et fabriqués à 100 % en France.

Nous vous entendons dans le cadre des réflexions de la mission sur la souveraineté numérique et technologique de la France et de l'Union européenne. Votre audition préludera utilement aux différentes tables rondes relatives à la commande publique que nous prévoyons d'organiser en janvier.

Je souhaite que vous nous présentiez votre entreprise, que vous nous fassiez part de votre regard sur la notion de souveraineté numérique. Je crois qu'elle n'est pas définie tout à fait de la même manière dans les différents pays européens. Je voudrais avoir votre avis sur la meilleure façon, pour les pouvoirs publics, de promouvoir cette souveraineté.

Nous écouterons avec beaucoup d'attention une courte présentation du marché des ordinateurs sur lequel vous êtes présent en France si vous souhaitez nous en faire une. Nous aimerions aussi connaître votre actualité pour 2021 et la façon dont la pandémie a pu impacter vos activités en 2020.

M. Philippe Latombe, rapporteur. Je me réjouis que nous auditionnions le dirigeant d'une PME qui propose une gamme d'ordinateurs conçus et fabriqués en France à 100 %. Nous avons en effet à cœur de rencontrer des acteurs privés développant des solutions technologiques souveraines afin qu'ils partagent avec nous leur regard de praticien sur le sujet.

Je voudrais d'abord savoir quel sens revêt pour vous la notion de souveraineté numérique. Ce concept, parfois rapproché de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et à ne pas subir les contraintes imposées soit par des acteurs publics comme les États soit par des acteurs privés comme les géants du web (GAFAM). Je voudrais savoir ce que vous pensez de la montée en puissance de cette thématique dans le débat public.

Il me semble également intéressant que vous nous indiquiez de quelle façon cet enjeu impacte votre activité en tant qu'entreprise développant une gamme d'ordinateurs autonome sur le plan technologique.

J'aimerais aussi revenir avec vous sur la façon dont les pouvoirs publics français ou européens peuvent concourir à promouvoir ou à protéger notre souveraineté numérique. Nous avons en effet auditionné des collectivités locales avec lesquelles nous avons abordé les enjeux de la commande publique. À votre échelle, qu'attendez-vous des acteurs publics ?

L'accès à la commande publique vous semble-t-il suffisant ? Nous sommes évidemment intéressés, le cas échéant, par les pistes de recommandations que vous pourriez nous suggérer sur ce point.

Enfin, nos travaux portent aussi sur la dimension technologique de la souveraineté numérique, qui est au cœur du plan de relance présenté par le Gouvernement. Je souhaite que vous nous fassiez connaître le regard que vous portez sur l'action des pouvoirs publics, aussi bien sur la partie du financement que sur la protection des savoir-faire d'une entreprise technologique. J'aimerais aussi que nous ayons un échange sur les secteurs technologiques au sein desquels il est selon vous indispensable de développer une autonomie afin d'éviter d'éventuelles ruptures d'approvisionnement en composants stratégiques en cas de crise. L'expérience de la crise de la covid pourra peut-être utilement nous éclairer.

M. Denis Psomiades, président-directeur général de CLESSE. Je vais vous répondre en trois temps, en expliquant d'abord pourquoi nous ne faisons actuellement pas de souveraineté numérique, ensuite comment il est difficile de se protéger dans le magma actuel des solutions proposées et enfin en détaillant les difficultés que nous rencontrons en essayant de faire de la souveraineté numérique.

CLESSE conçoit et fabrique depuis trente-cinq ans des équipements électroniques industriels et, depuis l'année dernière, un ordinateur 100 % français. Je tiens à m'excuser par avance pour les raccourcis que je devrai faire : le sujet très vaste et je serai donc succinct sur certains points.

Pourquoi s'intéresser à la souveraineté numérique ? Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique, écrit : « *Nous devenons vulnérables parce que nous sommes obligés d'avoir recours à du code que nous n'avons pas créé. Ce code est porteur de valeurs et de principes qui ne sont pas les nôtres, tant en termes de protection des données personnelles qu'en termes d'organisation du dialogue social ou d'évolution de nos sociétés*. » Le tableau est posé et la situation paraît très grave. Je note en particulier dans cette phrase les termes « vulnérables » et « obligés ». Il semblerait donc que notre vulnérabilité provienne d'une obligation, que nous n'ayons aucun moyen d'action.

Je prends quelques exemples concrets. Lise Charmel, société lyonnaise qui confectionne de la lingerie féminine, est aujourd'hui en redressement judiciaire à la suite d'une attaque par rançongiciel. Du fait que nous ne sommes pas souverains, cette société utilise un outil, en l'occurrence des ordinateurs, qui sont manifestement critiques pour son fonctionnement puisque c'est à la suite du rançongiciel qu'elle s'est retrouvée en redressement judiciaire. Ces outils ont été conçus par des gens qui n'ont pas les mêmes intérêts que nous. Si nous considérons n'avoir aucune solution alternative, les sociétés françaises sont condamnées, comme Lise Charmel, à être vulnérables aux rançongiciels. C'est un constat qui pose problème puisque cela commence à impacter nos sociétés. La confection, donc la mode, touche la société de manière générale et notre propre vision de l'avenir, de la vie et de la façon de vivre en France.

Mon deuxième exemple est le cas de la société Saint-Gobain qui a été un jour attaquée par un rançongiciel. Selon leurs publications, cela leur aurait coûté 250 millions d'euros. C'est un très gros chiffre que je veux mettre en rapport avec une étude universitaire selon laquelle réaliser un système d'exploitation (OS, *operating system*) coûterait environ 800 millions d'euros. Trois attaques de Saint-Gobain permettraient en gros de payer un système d'exploitation français donc souverain. Je ne suis pas vraiment d'accord avec le

calcul qui suit dans l'étude universitaire, indiquant que cela coûterait 12 euros par Français et ne serait donc économiquement pas rentable. Il faut savoir que les coûts informatiques dans une entreprise, en prenant tout en compte, sont de 2 000 à 5 000 euros par poste et par an. L'universitaire ajoute que le gouvernement français aurait des ambitions de souveraineté en matière de système d'exploitation, que ce n'est pas bien et que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) n'est heureusement pas d'accord.

Les grandes entreprises changent actuellement en moyenne un quart de leur parc informatique chaque année, de façon à le renouveler entièrement tous les quatre ans pour suivre l'évolution du matériel et des systèmes d'exploitation. En matière d'obsolescence programmée, je pense que ce domaine est quand même un peu sur le podium, surtout que nous savons aujourd'hui qu'il n'est pas nécessaire de faire évoluer ainsi les systèmes d'exploitation dans les entreprises.

Je passe à un autre exemple : dans une conférence disponible sur le site du Club de la sécurité des systèmes d'information régional (CLUSIR), un club de directeurs des systèmes d'information (DSI) lyonnais, présentée en partie par une représentante de la caisse primaire d'assurance maladie (CPAM), se trouve une liste non exhaustive des difficultés rencontrées par le service informatique de la CPAM, dont l'évolution non souhaitée des systèmes d'exploitation. L'un des exemples présentés est le fait qu'il est demandé à un certain nombre d'agents de venir un samedi pour rattraper un retard dans le traitement des dossiers occasionné par une surcharge de travail. Lorsqu'ils arrivent le samedi, le système d'exploitation se met à jour ce qui leur fait déjà perdre vingt minutes et, ensuite, l'outil logiciel qu'ils devaient utiliser n'est plus disponible après la mise à jour du système d'exploitation. Ce sont des coûts dont on parle rarement, beaucoup moins que des rançongiciels qui sont des accidents. Cet exemple n'est pas un accident, c'est un coût récurrent qui impacte les administrations et pas seulement. De ce fait, les entreprises ne peuvent pas atteindre le meilleur de leur performance. Les coûts entraînés par un tel phénomène, qui engendrent de plus des coûts de maintenance, sont liés uniquement à une évolution du matériel, et même ici uniquement du système d'exploitation, qui n'est pas souhaitée.

J'ai un dernier exemple très concret, celui de mon boulanger qui m'a dit ne détenir absolument aucune information confidentielle ou stratégique. Un jour, il passe par mail à son fournisseur de farine des commandes plus importantes que celles qu'il fait d'habitude pour une raison quelconque qui fait qu'il a vendu plus de pain que d'habitude. Il se trouve que tous les boulangers en Europe ont vendu plus que d'habitude et donc rachètent plus de farine. Ils envoient tous par mail des commandes à leurs fournisseurs. Nous voyons alors l'expression concrète du *big data* : il existe des sociétés dont le métier est de récupérer des informations anonymisées, de les traiter, d'en tirer des tendances et d'acheter des actions sur les marchés pour faire des gains financiers avant même que le travail ait été fait par le fournisseur et l'acheteur. Cette capacité à intervenir sur le marché du blé en l'occurrence et donc à en tirer des profits sur notre dos avant même que le travail ait été fait est un préjudice difficile à apprécier mais qui est réel quotidiennement, aujourd'hui, tant que nous n'avons pas la capacité de protéger la totalité de nos données, y compris celles de mon boulanger.

Voilà pourquoi il est nécessaire d'être souverain sur la totalité des données. La perte de souveraineté constitue du piratage et du sabotage d'entreprises. Le rançongiciel est du piratage lorsqu'il se contente de demander de l'argent et devient du sabotage lorsque nous ne parvenons pas à avoir les codes de déchiffrement. De plus, si le chiffrement était dormant depuis six mois, même les sauvegardes sont corrompues d'où des problèmes pour les

entreprises. C'est même parfois un assassinat lorsque les gens impactés se suicident. Ce n'est pas moi qui le dis mais une source de la gendarmerie nationale l'explique très clairement et ce n'est pas anecdotique. C'est donc très grave.

Comment se fait-il que, après cinquante ans d'informatique, nous en soyons toujours à avoir des problèmes de ce type ? Il est tout de même étonnant que nous ne parvenions pas à sécuriser les ordinateurs que nous utilisons. Il faut bien comprendre que, dans un ordinateur, tout passe par le système d'exploitation. Aucun logiciel ne peut fonctionner sans que les entrées et sorties de ce logiciel passent par le système d'exploitation : le clavier, l'ethernet donc internet, la souris, l'écran… Le code secret que vous tapez pour chiffrer un fichier que vous voulez sécuriser passe par le clavier donc par l'OS qui prend le code pour le donner à votre logiciel de chiffrement. Même lorsque vous installez un logiciel, c'est en fait le système d'exploitation qui installe le logiciel comme il a envie de l'installer.

Le problème est que les OS contiennent des portes dérobées – *back doors* – et des failles. Nous en découvrons régulièrement dans tous les OS. Vous devez donc avoir une entière confiance dans celui qui a fait l'OS et dans l'OS lui-même.

Or, aujourd'hui, ceux qui ont fait les OS n'ont pas les mêmes intérêts que nous. Ils défendent leur propre pouvoir d'achat, le pouvoir d'achat de leur pays, leur culture et tout le reste. Parfois, certains disent que les emplois qui en découlent nous permettent de travailler. Le problème est que ce sont des emplois précaires, pauvres, parce qu'ils dépendent de modifications non souhaitées qui provoquent des coûts de maintenance chez nous. Ces coûts de maintenance sont totalement dépendants du bon vouloir de ceux qui font les modifications des systèmes d'exploitation. Les entreprises françaises ont ainsi décidé de changer un quart de leur parc informatique chaque année et nous voyons bien le coût que représente le fait de changer un quart du parc alors qu'il n'y en a pas besoin fondamentalement.

Il existera donc toujours un différentiel de productivité entre les concepteurs des systèmes d'exploitation et ceux qui se contentent de les utiliser. Ce différentiel de productivité nous met toujours en difficulté commercialement.

Lorsque les amortisseurs d'une voiture sont fatigués, que faut-il faire ? Changer toutes les routes de France, les élargir, mettre des barrières pour que cette voiture puisse rouler ? Vaut-il mieux changer les amortisseurs de la voiture ? Aujourd'hui, la meilleure solution serait d'avoir un ordinateur de confiance qui permettrait d'éviter toute cette charge.

Actuellement, environ 60 000 personnes travaillent dans la cybersécurité en France. Ces 60 000 personnes dans la cybersécurité ne produisent rien, c'est une charge pour les entreprises, pour toutes les entreprises françaises et européennes. Pourtant, lorsque nous posons la question à un directeur des services informatiques (DSI), il répond qu'il n'existe pas d'alternative. Il a raison, il n'existe pas d'alternative et nous retrouvons ce que dit Bernard Benhamou : « *nous sommes obligés* ».

Nous avons proposé une alternative. Nous sommes français et nous avons les mêmes intérêts que tous les Français. Nous avons conçu un « *hardware* », un OS et des logiciels. Nous avons vendu le tout à des industriels de la région lyonnaise pour démontrer la faisabilité. En effet, lorsque nous avons dit que nous pouvions le faire voici six ans, personne ne nous a crus, en particulier pas la Banque publique d'investissement (BPI). Nous avons donc décidé d'investir sur fonds propres en comprenant que, tant que nous n'aurions pas démontré la

faisabilité, il serait impossible d'en parler. Il existe ainsi aujourd'hui des entreprises qui fonctionnent quotidiennement avec des systèmes 100 % français.

Nous avons proposé le Business Computer à des DSI de grandes entreprises et à des administrations, dans le but de faire baisser le coût de la facture informatique de façon générale. Nous avons alors rencontré ce que nous appelons le « syndrome du DSI ». De quoi s'agit-il ?

Lorsqu'un directeur général (DG) d'une entreprise parle à son directeur commercial, il utilise des termes tels que « marge », « part de marché » que tout le monde connaît ce qui leur permet de se comprendre. Lorsqu'un DG parle à un DSI, le problème est qu'ils ne parlent pas du tout la même langue. Le DSI parle de machine virtuelle, d'architecture trois tiers, de VPN, d'agrégateur de liens, de noyau… et le DG, ne comprenant même pas la langue, donne à son DSI l'entière responsabilité de la gestion informatique de l'entreprise. Comme le DSI est responsable de tout du fait que personne ne comprend ce qu'il fait, il choisit des solutions standard pour que, en cas de problème, il ne lui soit pas reproché d'avoir utilisé autre chose, tout en connaissant parfaitement les risques encourus.

Lorsque nous nous adressons à un DSI pour lui proposer un système de confiance français, la phrase que nous entendons systématiquement est : « *Je ne peux pas introduire dans mon entreprise un matériel atypique car, au moindre problème, je prendrais le risque de me faire licencier.* » Les choix en matière de souveraineté numérique ne sont donc pas guidés par les intérêts des entreprises mais par un problème d'habitude, peut-être parfois un manque de compétences compréhensible car l'informatique est un domaine très compliqué.

Si les directeurs généraux étaient conscients des risques, toute une part de la numérisation des entreprises ne se ferait pas. Par exemple, nous voyons aujourd'hui dans les entreprises des broyeurs de documents ; toute l'information est dans le *cloud* ce qui est une incohérence totale, donne un faux sentiment de sécurité aux gens et rend encore plus dangereuse l'utilisation de l'informatique dans certains cas de figure.

Nous en avons conclu que c'était aux institutions que revenait la charge d'aider les différentes composantes de la société à jouer collectif sur le sujet, à cautionner des solutions informatiques françaises comme le gouvernement américain l'a fait pour IBM, Facebook, Google et Amazon. C'est tous ensemble que nous pouvons renverser la tendance.

Nous avons donc contacté un ministère pour proposer notre Business Computer. Nous avons été mis en relation avec le responsable informatique du ministère qui m'a répondu ne pas pouvoir acheter un système français pour équiper son ministère s'il n'est pas certifié par l'ANSSI. Nous retombons donc sur le syndrome du DSI qui veut du matériel standard, certifié et ne le fait sinon pas rentrer dans l'entreprise. Nous ne pouvons donc pas créer en France une solution informatique innovante puisque l'ANSSI demande de faire un gros chiffre d'affaires pour accepter d'ouvrir un dossier de certification et que, pour faire un gros chiffre d'affaires, il faut être certifié. Il n'est pas possible d'entrer dans le système.

J'ai évoqué auprès de ce fonctionnaire du ministère le décret n° 2018-1225 qui permet à l'administration d'acheter une start-up hors cadre des marchés publics pour réaliser une preuve de concept. Ce décret tombe à pic ; il est très bien fait et permet de lever une barrière technique qui a sa justification puisque le code des marchés publics est très utile également. Le responsable informatique du ministère m'a répondu : « Ce n'est pas mon problème ! » Si ce n'est pas le problème de celui qui décide sous la tutelle du veto de l'ANSSI, il n'est pas

possible aujourd'hui, en France, de proposer une véritable souveraineté numérique, du fait des institutions.

Il est clair que l'informaticien et l'ANSSI ne doivent pas détenir un pouvoir de veto sur le déploiement de solutions innovantes, françaises et, en définitive, favoriser en creux le déploiement de solutions étrangères qui ne sont pas plus certifiées et pas certifiables. C'était le sens du décret, décret que personne ne met en œuvre. Le simple fait que la solution soit française devrait au minimum susciter de l'intérêt et ce n'est pas le cas.

Nous n'en sommes pas restés là. Nous avons un client dans le secteur de la dissuasion nucléaire. Je vous rappelle qu'il s'agit de bombes atomiques et de missiles. Ce client est audité régulièrement par l'ANSSI. Nous lui avons proposé notre matériel. Il nous a répondu, selon le même syndrome du DSI, qu'il ne peut pas proposer nos produits à sa direction ni à ses clients parce qu'il a peur que l'ANSSI ne certifie pas leur système s'il contient nos solutions. Cela signifie que, aujourd'hui, en France, nous utilisons pour la dissuasion nucléaire française des systèmes étrangers, pas certifiables du tout puisque nous n'avons pas accès aux sources des programmes, et que, pour faire de la bureautique dans les ministères, un système français qui pourtant serait certifiable n'est pas accepté. Je vous laisse seuls juges.

La doctrine de l'ANSSI n'est actuellement pas compatible avec le déploiement de solutions innovantes de sécurité françaises. L'ANSSI dispose d'un pouvoir de décision sur des choix de marchés stratégiques sur lesquels la France doit concentrer ses efforts. Or, ce type de choix ne fait pas partie des compétences des informaticiens. Ils ne sont pas formés pour. La doctrine de l'ANSSI consistant à dire que les Américains ont trop d'avance et donc que c'est peine perdue d'essayer de prendre des parts de marché dans le secteur des ordinateurs souverains est une erreur stratégique grave pour la France et l'Europe. Vous ne pouvez pas dire aux Français et à des chefs d'entreprise que nous abandonnons avant même d'avoir essayé la conquête d'un marché européen de 200 à 300 milliards d'euros. C'est tout simplement inaudible.

Tout ceci contraste avec la volonté manifeste de souveraineté du Président de la République dans pratiquement tous ses discours. Cela contraste également avec les injonctions de Bruno Le Maire envers les entreprises auxquelles il demande en substance de faire comme les grandes entreprises étrangères qui rencontrent un grand succès. Comment faire, puisque toutes les entreprises françaises partent avec un handicap que l'ANSSI, par idéologie, ne cherche pas à combler ?

Il faut comprendre que le système d'exploitation et le « *hardware* » sont la clé de voûte de toute la filière. Beaucoup de chefs d'entreprise en France l'ont très bien compris. Le Collectif des 200 qui s'est créé le crie haut et fort. La suprématie américaine s'est créée par exemple parce que les fabricants d'OS ont choisi des puces électroniques américaines pour équiper les ordinateurs américains. Si nous créons demain en France une véritable filière d'informatique souveraine, nous pourrons choisir par exemple des composants de STMicroelectronics ce qui lui permettra de faire beaucoup plus de chiffre d'affaires. Grâce à ce chiffre d'affaires, peut-être STMicroelectronics auraient-il pu avoir les moyens de racheter ARM, ce qui n'a pas été le cas. C'est ainsi que fonctionne une filière. En partant de l'ordinateur et de l'OS, nous finançons toute la filière.

En concevant vous-même un OS, vous avez six mois d'avance sur tous les autres développeurs qui l'utilisent. C'est ce qui a permis aux Américains de proposer dans des

solutions standards du marché des fonctionnalités avec six mois d'avance sur tous les autres. Dans le monde de l'informatique, cet avantage de six mois est fondamental.

Celui qui fait l'OS, par la force des choses, choisit également par exemple la langue dans laquelle la documentation d'utilisation du système d'exploitation est écrite. Que ce soit clair, aujourd'hui, pour les jeunes Français, l'anglais est du chinois donc ils sont forcément pénalisés en faisant face à deux problèmes différents, l'informatique et la langue, deux pédagogies différentes, deux temps différents. Disposer d'une documentation en français pour apprendre à coder permettrait d'être beaucoup plus productif dans les entreprises et, par effet différentiel, d'autres le seraient moins. Il faut jouer collectif, travailler ensemble comme le font très bien les Allemands et les Américains. Ce n'est pas le cas en France.

J'ajoute que des économistes disent souvent à la radio que, à chaque bouleversement technologique, il y a toujours des gagnants et des perdants mais que, cette fois, nous n'avons pas vu les gagnants. Ils sont étonnés que la croissance soit absente. En fait, ils ne regardent pas bien. Aux États-Unis, la filière informatique représente 1 000 milliards de dollars de chiffre d'affaires et un million d'emplois directs.

La marge financière des entreprises françaises est aujourd'hui siphonnée par les coûts des solutions informatiques étrangères. Ce sont des coûts totalement prohibitifs et non justifiés. Nous sommes dans un piège et il est nécessaire de retourner la situation tout de suite. Les systèmes informatiques sont beaucoup trop sensibles et font courir un risque systémique grave à toutes nos entreprises et à notre société.

Il est urgent de changer d'objectif, de passer d'un objectif de toujours plus à un objectif de résilience de nos systèmes. Il est donc nécessaire de disposer d'un *hardware* et d'un OS conçus pour défendre nos intérêts économiques, respecter nos valeurs européennes, notre vision de l'avenir, notre indépendance, en bref, notre souveraineté.

M. le président Jean-Luc Warsmann. Avez-vous une idée du montant d'investissements que représente le développement de ce *hardware* et de cet OS français ou européens ?

M. Denis Psomiades. Nous avons créé un OS et un *hardware*. Ce *hardware* est également 100 % CLESSE. Nous l'avons mis sur le marché et vendu à deux entreprises de la région lyonnaise. Cet OS existe et nous ne demandons aucun financement pour le faire. Nous demandons seulement l'aide des pouvoirs publics, par exemple en aidant cette entreprise qui travaille sur la dissuasion nucléaire française à accepter les systèmes souverains que nous proposons déjà.

M. le président Jean-Luc Warsmann. Vous nous avez décrit la position de l'ANSSI. Cette position vous a-t-elle été communiquée par écrit ? Existe-t-il un mode opératoire de l'ANSSI qui exige qu'une solution dégage un certain montant de chiffre d'affaires pour être agréée ?

M. Denis Psomiades. C'est la réponse qui nous a été faite plusieurs fois.

M. le président Jean-Luc Warsmann. A-t-elle été faite par écrit ?

M. Denis Psomiades. Non, pas par écrit, c'est l'expérience des différents appels à idées ou appels d'offres qui ont eu lieu récemment et d'une communication téléphonique très récente.

M. le président Jean-Luc Warsmann. Souhaitez-vous évoquer un autre sujet ?

M. Denis Psomiades. Je reprends rapidement les questions qui avaient été posées au début de l'audition.

En ce qui concerne notre actualité pour 2021, le déploiement des solutions Business Computer dépend aujourd'hui des pouvoirs publics. Sans leur aide, nous retrouverons le syndrome du DSI.

La crise de la covid-19 nous a impacté car l'année est marquée par des annulations de commandes ou de marchés, notamment dans l'aéronautique.

S'agissant de la façon dont les acteurs publics peuvent concourir à l'émergence de la souveraineté numérique, il faut redéfinir la doctrine en matière de cybersécurité et régler le problème à la source. Il faut aussi jouer collectif, ce qui n'est pas le cas en France.

La question de savoir si la commande publique est suffisamment orientée vers des solutions technologiques françaises est très complexe. Cette réponse nécessite des nuances et il m'est difficile de répondre rapidement.

Le plan de soutien aux entreprises technologiques est actuellement inaccessible pour les petites structures. Les objectifs sont souvent peu pertinents. Dans le cas de la 5G par exemple, l'intérêt stratégique de la développer est douteux et, dans tous les cas, il ne faut la développer qu'à condition qu'elle soit française. Le monde a changé et nous ne travaillons plus avec les deux autres continents. Il est nécessaire que nous défendions nos propres intérêts.

Dans le cas du secteur spatial, qui se fait actuellement dépasser très clairement par les Américains, les choix effectués ont été mauvais et le sont toujours. Je connais d'assez près ce secteur puisque nous avons eu l'occasion d'y travailler.

Sur l'approvisionnement en composants critiques, il serait effectivement intéressant de regarder de près les réseaux de portes programmables *in situ* (FPGA, *Field-Programmable Gate Array*). Un financement a déjà été mis en œuvre et porte ses fruits. Il faut penser aussi aux mémoires, aux technologies de gravure à pas fin que STMicroelectronics a abandonnées pour des questions de coûts. Ce sont des usines à quelques milliards. Je pense que, dans le plan européen de 750 milliards d'euros, la mise en œuvre d'une usine de gravure de composants à pas fin serait un bon investissement. Nous ne sommes plus capables de le faire en Europe depuis longtemps. Pourtant, cela me paraît fondamental pour avoir des composants, notamment des microprocesseurs, performants et efficaces à l'avenir.

En ce qui concerne l'approvisionnement de CLESSE, nous sommes sous le coup d'un possible veto des Américains sur certains composants du fait des *International Traffic in Arms Regulations* (ITAR), ce qui n'est pas acceptable pour les entreprises. Vous pouvez acheter aujourd'hui un composant qui deviendra ITAR demain ce qui fait que vous ne pourrez plus l'exporter. Ces contraintes sont insupportables et il faut que tous ces composants soient fabriqués en Europe pour ne pas avoir à subir des contraintes ITAR.

Il existe aussi des restrictions d'exportation liées à l'utilisation de nouveaux formats de protocoles qui ont été créés aux États-Unis et nous font arriver en retard sur certains marchés alors que nous sommes tout à fait capables de créer nos propres protocoles et nos propres composants.

M. le président Jean-Luc Warsmann. Pourriez-vous décrire plus précisément en quoi nous ne jouons pas assez collectif en France ?

M. Denis Psomiades. Lorsque nous nous adressons au DSI d'une grande entreprise française comme Saint-Gobain par exemple, il faudrait qu'il soit au moins capable de nous ouvrir la porte de la discussion. Pour qu'il le fasse, compte tenu de l'appréhension à laquelle nous nous heurtons sur les systèmes français, il faudrait que la composante publique soit présente, qu'elle donne caution d'une manière ou d'une autre, pas financièrement mais simplement en encourageant ce DSI à utiliser une solution souveraine française existante pour qu'il ne se sente pas coupable de le faire. Ce n'est même pas une question d'argent ; il s'agit de se mettre autour de la table et d'en discuter.

De plus, l'ANSSI dit ouvertement – ce sont des écrits qui se trouvent sur internet – ne pas encourager le fait de choisir une solution souveraine. Le directeur général de l'ANSSI l'a dit dans un discours en 2016 et une communication téléphonique récente me confirme que la doctrine est toujours la même.

Il faut donc d'un côté enlever les freins et de l'autre mettre les gens autour de la table pour créer un collectif ou un groupement d'intérêts économiques qui permette aux DSI, sans prendre le risque de perdre leurs postes, d'accepter des solutions françaises. Le cas de la dissuasion nucléaire est symptomatique. Il est évident que cela devrait se faire et nous avons pourtant ce blocage.

M. le président Jean-Luc Warsmann. Je vous remercie pour ces avis dont nous tirerons profit au maximum, pour votre liberté de ton et pour les éléments très concrets que vous avez apportés. Je vous souhaite beaucoup de succès et, si la mission peut vous aider à lever quelques blocages, nous essaierons de le faire.

La séance est levée à 11 heures 45.

Membres présents ou excusés

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

Réunion du jeudi 17 décembre 2020 à 11 heures

Présents. - M. Philippe Latombe, M. Denis Masséglia, M. Jean-Luc Warsmann

Excusés. - Mme Frédérique Dumas, M. Jean-Michel Mis