ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la conférence des présidents sur la résilience nationale

– Audition de M. Olivier Kempf, chercheur associé, Fondation pour la recherche stratégique (FRS) et de M. Julien Nocetti, chercheur associé, Institut français des relations internationales (IFRI) 2

– Présences en réunion 10

Mercredi
22 septembre 2021
Séance de 16 heures 30

Compte rendu n° 20

SESSION EXTRAORDINAIRE DE 2021

Présidence de
M. Alexandre Freschi,
Président de la mission d'information

ASSEMBLÉE NATIONALE

MISSION D'INFORMATION DE LA CONFÉRENCE DES PRÉSIDENTS SUR LA RÉSILIENCE NATIONALE

Mercredi 22 septembre 2021

La séance est ouverte à seize heures trente

(Présidence de M. Alexandre Freschi, président de la mission d'information)

M. le président Alexandre Freschi. Nous recevons deux chercheurs dont les travaux ont partie liée avec les risques cyber : M. Olivier Kempf, chercheur associé à la Fondation pour la recherche stratégique (FRS) ; intervenant dans plusieurs grands établissements d'enseignement supérieur et exerçant une activité de conseil, il a publié l'an dernier un article intitulé « *Cybersécurité et résilience : les grands oubliés des territoires* » ; M. Julien Nocetti, enseignant-chercheur à l'académie militaire de Saint-Cyr Coëtquidan et chercheur associé à l'Institut français des relations internationales (IFRI), chercheur au centre géopolitique de la datasphère (GEODE) et directeur de la chaire gouvernance du risque cyber à Rennes School of Business.

M. Olivier Kempf, chercheur associé, Fondation pour la recherche stratégique (FRS). Je suis également fondateur et vice-président de l'Institut national pour la cybersécurité et la résilience des territoires. Nous avons rapproché ces notions de résilience et de cybersécurité et celle de territoire, car ces espaces ne sont pas épargnés par les risques systémiques qui se multiplient. Si la résilience des territoires était surtout appréhendée sous le prisme des calamités naturelles, de nouvelles menaces systémiques pouvant affecter la résilience des territoires se manifestent avec une ampleur particulière, en particulier depuis les derniers mois : pensons à la pandémie, aux chocs climatiques ou aux risques cyber. Une sorte de « pandémie cyber » s'est même abattue sur nos territoires, nos entreprises, nos collectivités, nos concitoyens, qui se traduit par une véritable explosion des cyberagressions – terme que je préfère à celui de cyberattaques – qui me semble plus approprié aux usages militaires – reposant sur deux principaux vecteurs : le rançonnage, qui est désormais bien connu ; le « minage » clandestin des ordinateurs visant à extraire des *bitcoins* et autres cryptomonnaies ; ce phénomène ne doit pas être négligé.

Ces cyberagressions affectent de larges pans de l'activité et affichent une croissance à la fois quantitative – plus personne ne peut considérer qu'il est trop petit pour être agressé – et qualitative – nous observons une industrialisation et une élévation du niveau des agressions, même si la plupart d'entre-elles frappe surtout les premiers échelons de défense. L'image du pirate informatique capable de casser le code de la CIA depuis son garage de Saint-Pétersbourg ou de San Francisco relève désormais du mythe. Les pirates informatiques se sont professionnalisés et regroupés pour intensifier leurs activités. Ils peuvent tirer parti de la croissance continue du cyberespace, dont l'extension est liée aux vagues successives de révolutions informatiques – la transformation numérique étant la dernière en date – que nous connaissons depuis quarante ans. Ces acteurs bénéficient également de la multiplication des usages du numérique – que la pandémie a d'ailleurs accélérée à travers la généralisation du travail à distance.

Nous constatons par ailleurs un accroissement de la cyberconflictualité, qui relève du niveau politique et géopolitique. Il ne saurait cependant être question de « cyberguerre », dans la mesure où cette conflictualité se maintient en deçà d'un seuil de létalité dont les contours restent à définir. La difficulté d'attribuer les actions dans l'espace cyber à un agent ou à un commanditaire déterminé permet une multiplication des initiatives, qui perturbent nos alliances traditionnelles. Nos amis sont peu nombreux, puisque tout le monde avance masqué, sans connaître réellement les actes de l'autre. Tout le monde s'espionne. Dans la mesure où cette cyberconflictualité non létale n'impressionne ni les populations ni les dirigeants, il est difficile de l'entraver.

M. Julien Nocetti, chercheur associé, Institut français des relations internationales (IFRI). J'évoquerai d'abord deux notions clés, celle de risque et celle de dépendance, en me concentrant notamment sur la composante géopolitique du risque cyber et sur ses implications pour la France et l'Europe.

Celui-ci a pris rang parmi les principaux risques systémiques identifiés par les grandes institutions internationales et européennes, en sus des risques liés notamment à l'instabilité financière, au changement climatique et aux menaces pandémiques. Dans ce cocktail détonnant, il est parfois difficile de situer le risque cyber au sein d'une nomenclature des menaces. Le cyber contribue au brouillage des distinctions traditionnelles entre civil et militaire, temps de guerre et temps de paix, affaires intérieures et politique étrangère.

La maîtrise du cyber tend à devenir un attribut de la puissance des États, tout en participant de la relativisation de la place de ces derniers dans la conduite de relations internationales qui semblent engagées dans un processus de privatisation. En effet, alors même que certains analystes peuvent être enclins à maintenir une approche centrée sur le rôle des États, les conflits cyber sont bien davantage le fait d'acteurs privés, éventuellement d'entreprises, que de diplomates ou d'autres agents publics.

L'approche du risque cyber met traditionnellement l'accent sur la criminalité. Jusqu'à une date récente, l'on assimilait la cybercriminalité au bas du spectre des menaces, à tel point que les arsenaux et doctrines cyber élaborés par les États plaçaient l'enjeu criminel au second plan. La crise du covid-19 a rappelé l'acuité de ce risque, qui a pris une ampleur différente à l'heure du recours généralisé au télétravail et de la satellisation des données critiques des entreprises : au lieu d'être stockées principalement sur des serveurs internes, ces données sont réparties, diffusées auprès des collaborateurs, des prestataires ou encore des fournisseurs. La cybercriminalité est donc devenue un enjeu majeur des préoccupations des décideurs.

L'extorsion de fonds et de données par le truchement du numérique est devenue une activité industrielle qui engendre en un temps limité des profits importants pour les pirates et les réseaux. Le versement des rançons en cryptomonnaie rend de surcroît plus difficile le traçage des fonds et l'identification des auteurs. Le logiciel de rançonnage ou « rançongiciel » est devenu la mère des cyberattaques, et s'apparente au gré de son développement à un *business* « comme les autres », avec ses règles propres et sa division du travail entre développeurs, vendeurs et exécutants. Il s'agit d'une industrie hautement professionnalisée et globalisée, comme en témoigne notamment l'attaque menée au printemps dernier par le groupe cybercriminel DarkSide contre l'entreprise Capital Pipeline. DarkSide pratique le rançonnage sous forme de prestation de services – *ransomware as a service* – : ses opérateurs font appel à d'autres acteurs pour conduire les attaques, moyennant un partage du butin tel que, selon certaines estimations,70 à 90 % des gains reviennent à l'auteur de l'attaque. Nous

assistons ainsi à une démocratisation des outils malveillants et à une multiplication des acteurs de la cybercriminalité.

Plusieurs facteurs contribuent à expliquer la recrudescence des rançongiciels, dont deux soulèvent des enjeux particuliers. D'une part, l'économie politique de la cybercriminalité – un modèle d'affaires très lucratif – est largement hébergée en Russie, et plus généralement dans l'espace post-soviétique, ce qui a des conséquences évidentes sur les relations internationales. D'autre part, l'investissement des différentes organisations pour leur cybersécurité reste insuffisant, alors même que l'évolution des modes de travail et la circulation des données suscitent et accroissent leur vulnérabilité aux risques numériques.

Trois pistes d'action sont à envisager pour lutter contre les rançongiciels.

Je pense d'abord au démantèlement de l'écosystème cybercriminel, qui consiste notamment à effacer les serveurs hébergeant des forums utilisés par les groupes cybercriminels et à réguler les plateformes d'échange de cryptomonnaie. Par exemple, le Trésor américain a récemment sanctionné la plateforme Suex pour son implication dans le blanchiment de fonds résultant de cyberattaques. Il s'agit d'empêcher la réalisation de profits par le biais de rançongiciels.

Le deuxième axe consiste à répondre aux enjeux géopolitiques qui sous-tendent ces risques, comme le président des États-Unis Joe Biden s'y est efforcé cet été lors de sa rencontre à Genève avec le président russe Vladimir Poutine. À l'issue de ce sommet, la Maison-Blanche a adressé un avertissement sous forme de ligne rouge en dévoilant une liste de seize infrastructures américaines critiques contre lesquelles toute cyberattaque ferait l'objet de rétorsions et de représailles. L'avenir nous montrera si cette ligne rouge sera respectée.

Le troisième axe concerne le renforcement de la coopération internationale entre les services de police spécialisés dans la lutte contre la cybercriminalité ; les réussites de ces services ne sont guère médiatisées, mais leur action s'avère de plus en plus cruciale. Rappelons, pour apprécier l'ampleur du phénomène, que cinq millions de nouveaux virus informatiques sont détectés chaque semaine.

Après avoir évoqué le bas du spectre, je parlerai également de l'aspect géopolitique de la menace cyber, qui concerne particulièrement la France, qui figure parmi les dix États les plus ciblés par les cyberattaques. Celles-ci prennent des tournures de plus en plus militarisées et offensives, comme l'ont montré les affaires SolarWinds et Microsoft Exchange, qui ont suscité de vifs débats au sein de l'appareil d'État civil et militaire américain. Ce contexte n'est pas celui d'une cyberguerre, mais celui d'un état de conflictualité latente. Le cyber constitue avant tout une ressource géopolitique qui permet à certains États contestant l'hégémonie américaine d'engager un rapport de force asymétrique à faible coût financier et humain. Pour l'heure, les conséquences stratégiques demeurent marginales, en raison de la difficulté d'engager des représailles, de la diffusion très large d'outils et de tactiques malveillants et de l'enjeu de l'attribution, marqué par une difficulté à établir une doctrine harmonisée au niveau européen, sachant que la menace cyber se couple à l'enjeu informationnel tel que pratiqué par d'autres acteurs géopolitiques. Les risques d'escalade sont désormais bien identifiés, avec des doctrines plus offensives. Leur mise en œuvre est cependant en difficulté compte tenu des contours relativement flous entre ce qui relève de l'appât du gain, de l'espionnage ou de l'acte de guerre.

M. Thomas Gassilloud, rapporteur. Pour débuter sur une question géopolitique globale, pouvez-vous d'abord préciser quel est le niveau de dépendance du fonctionnement de l'internet aux autorités américaines ? Par ailleurs, savez-vous si certains pays cherchent à se soustraire à cette dépendance ?

M. Olivier Kempf. L'internet au sens large, qui constitue une partie du cyberespace, a été conçu et construit par les Américains. Le rôle éminent des États-Unis s'est d'abord manifesté en matière de réglementation et de standardisation, puis par la mise en place de géants du numérique. Cela dit, nous observons une autonomisation croissante de la Chine à l'égard de ce système mondial. La Chine est probablement le seul pays au monde à être parvenu à bâtir une cyber-souveraineté pour les trois couches du cyberespace, que sont respectivement: la couche physique, qui comprend les équipements physiques et notamment les infrastructures : la Chine n'est pas tout à fait souveraine pour son approvisionnement en semi-conducteurs, mais elle l'est assurément pour le fonctionnement de ses infrastructures, comme le montre le déploiement de ses propres réseaux de câbles ; la couche informationnelle et logicielle, qui comprend les codes et les protocoles : les restrictions d'emploi de certains outils informatiques américains comme Google, Amazon ou LinkedIn sont le corollaire de cette recherche d'indépendance en matière de logiciels ; la couche sémantique, qui comprend les données en circulation : à titre d'exemple, 47 des 50 sites internet les plus fréquentés en France sont d'origine américaine, contre seulement 3 des 50 sites les plus fréquentés en Chine.

La recherche par la Chine d'une souveraineté numérique, trouve un écho dans la stratégie d'autres pays, qui développent toutefois des politiques moins complètes faute de moyens : c'est notamment le cas de la Russie, de l'Iran et de la Corée du Nord. D'autres États réputés plus coopératifs affichent des stratégies curieusement semblables, comme la Géorgie – qui profite des spécificités de sa langue et de son alphabet – ou encore Singapour. La fragmentation lente et continue d'internet transforme progressivement cet espace mondial en un ensemble de plaques interconnectées qui ont tendance à se séparer, comme autrefois la Pangée, le continent unique dont procèdent ceux que nous connaissons.

Un troisième acteur doit également être pris en compte, à savoir les entreprises privées que sont Google, Amazon, Facebook, Apple et Microsoft – les GAFAM. ¨Au cours de leur développement, marqué notamment par la constitution de réseaux autonomes de câbles sous-marins, les acteurs privés perturbent la lecture classique de la géopolitique centrée sur les États et accentuent la fragmentation du cyberespace en général et de l'internet en particulier.

M. Julien Nocetti. Je reviendrai brièvement sur la Chine et la Russie, que nous avons parfois tendance à associer, en insistant sur ce qui les différencie. La Chine a rapidement bâti une stratégie d'autarcie technologique physique et logicielle, couplée à une vision précise de l'ordre international et des valeurs qu'elle entend diffuser. Nous en voyons l'illustration dans le projet des nouvelles routes de la soie porté par Pékin, qui comprend le déploiement d'infrastructures numériques et technologiques dans le cadre d'une stratégie d'exportation de son modèle idéologique et politique. La séduction de ce modèle chinois s'étend à de nombreux acteurs, y compris en Europe.

De son côté, la Russie n'a jamais été tout à fait étanche en matière technologique et numérique, malgré la multiplication des lois tendant à garantir la souveraineté de la Russie sur l'internet et des projets spectaculaires de verrouillage interne. En dépit de certaines déclarations de dirigeants russes, Moscou est encore très dépendant de serveurs situés à l'étranger, puisque 55 % des données des citoyens russes sont hébergées hors de Russie.

Malgré ces limites, la stratégie russe suscite l'attention, car elle n'est pas sans rapport avec la vision précise qu'ont les dirigeants russes de la place de leur pays dans le concert des nations : la mise en œuvre d'une stratégie numérique autonome permet aussi d'asseoir cette prétention à un rayonnement mondial.

Nos dépendances vis-à-vis des États-Unis sont évidentes, bien documentées et quasiment complètes, sur l'ensemble des couches du cyberespace. Je pense d'abord à notre dépendance vis-à-vis des câbles sous-marins américains, dont nous n'avons que tardivement pris conscience. Le marché câblier mondial est très complexe : sa structuration épouse plus ou moins le réseau télégraphique constitué au XIX^{e} siècle entre la Grande-Bretagne et les États-Unis. Les enjeux capitalistiques que soulève son développement sont étroitement imbriqués avec des enjeux de souveraineté. Google et Facebook conduisent ainsi des stratégies très offensives vis-à-vis de l'Europe et de l'Afrique, mais aussi de l'Asie du Sud-Est, dans des eaux au cœur des rivalités internationales. Notre dépendance s'observe aussi dans la couche logicielle du cyberespace, au vu de la place significative prise par les plateformes systémiques et ubiquitaires des GAFAM. Il existe d'ailleurs un dynamisme de ces acteurs favorisé par leur puissance financière et humaine qui leur permet de capter des ressources. L'extraterritorialité du droit américain sert également leurs intérêts. Tant que nous n'aurons pas trouvé, en Europe, des moyens de lutter contre cette extraterritorialité, notre potentiel d'action demeurera limité.

M. Olivier Kempf. Au-delà des câbles sous-marins, l'acteur privé qu'est Facebook déploie toute une galaxie de microsatellites à destination des acteurs privés que sont les citoyens et les entreprises du monde entier. La stratégie de cette entreprise n'est pas nécessairement alignée sur celle de Washington.

Pour illustrer notre dépendance, on peut rappeler les conséquences de l'intégration des données publicitaires de la messagerie instantanée WhatsApp avec celles de Facebook. Les usagers qui se sont désabonnés de ces services ne disposaient que de peu d'alternatives : parmi les plateformes comparables, rappelons que l'application Signal est éditée par une fondation de droit américain, par conséquent soumise au *Patriot Act* et au *Cloud Act* ; Telegram est un logiciel d'inspiration russe dont le siège social est à Abu Dhabi. De quelles garanties de sécurité dispose-t-on dans le cas d'une application basée à Abu Dhabi ? Peu d'usagers ont finalement opté pour un logiciel de messagerie instantanée gratuit d'origine européenne, tel que l'outil français Olvid, qui présente toutes les garanties de sécurité offertes par le cadre juridique européen. Au risque de paraître militant, je pense que ces initiatives doivent être encouragées pour nous départir de ces dépendances extérieures.

M. Thomas Gassilloud, rapporteur. Nous avons d'ailleurs échangé, avec le directeur interministériel du numérique (DINUM), sur la possibilité d'étendre le logiciel de messagerie instantanée de la fonction publique – Tchap – à l'ensemble des citoyens français ou européens, selon un portage restant à déterminer.

Si l'on revient à l'échelle des territoires, j'ai noté que monsieur Kempf a publié une note intitulée « Cybersécurité et résilience : les grands oubliés des territoires ». Qu'est-ce qui vous a conduit à choisir un titre si fort et percutant ?

M. Olivier Kempf. Il y a deux ans, nous constations que d'importants efforts avaient été consentis par les autorités nationales et européennes en matière de cybersécurité. Nous relevions aussi que le niveau inférieur du maillage administratif français – correspondant aux collectivités territoriales et aux circonscriptions administratives de proximité – était le grand

oublié de cette politique. Pourtant, les acteurs présents dans les territoires – collectivités publiques, syndicats mixtes, PME-PMI, professionnels indépendants – manipulent aussi des données sensibles. Ceux-ci ont parfois recours à des prestataires informatiques qui ne bénéficient pas toujours d'un label attestant leur compétence : cela témoigne d'un manque d'attention de ces acteurs à leur sécurité informatique. Beaucoup d'employeurs ont subitement généralisé le télétravail durant la pandémie et ont ensuite été confrontés à une vague de rançonnage. À ce manque de prise de conscience s'ajoute un défaut de partage de bonnes pratiques entre acteurs, moins dans le but d'adopter une réponse uniforme que de mettre en œuvre des réponses adaptées à chacun sur le fondement de ce qui existe et fonctionne pour certains acteurs.

Ces enjeux devraient être partagés par l'ensemble des acteurs du territoire, au-delà des seules collectivités publiques. Il s'agit de sensibiliser et de former ces différents acteurs, dans le but d'accroître leurs ressources en matière numérique. Compte tenu du coût que représente pour une commune ou une PME l'embauche d'un responsable de la sécurité des systèmes d'information (RSSI), titulaire d'une formation de niveau bac+5, des emplois de RSSI de proximité, occupés par des personnels légèrement moins qualifiés, pourraient être créés. Nous devrions également évaluer l'hypothèse d'un partage d'emplois dans le cadre de partenariats public-privé ou de groupements d'employeurs.

Dans le cadre de la réflexion sur les attributions à l'échelon départemental, peut-être devrions-nous transférer la compétence cyber aux départements de manière à permettre une prise de conscience, une animation et un partage des innovations de proximité fondées sur la réalité des territoires.

M. le président Alexandre Freschi. Vous dessinez un tableau extrêmement préoccupant, puisque vous affirmez que nous sommes en conflit avec tout le monde, que tous les acteurs avancent masqués et que nos alliances traditionnelles en souffrent. Dans ce contexte de vulnérabilité accrue à toutes les échelles, quels scénarios envisagez-vous pour faire face à des attaques massives ou ciblées ?

M. Olivier Kempf. D'abord, je pense qu'il convient d'imposer des obligations en matière de cybersécurité aux éditeurs de logiciels. Lorsque j'étais moi-même *Chief Data Officer* (CDO) de l'armée de terre, j'avais à la fois la responsabilité de libérer la circulation des données et de protéger leur exploitation. De leur côté, les *start-up* ne cherchent généralement qu'à libérer l'utilisation des données, sans se préoccuper des enjeux de sécurité que soulève leur exploitation. De nombreux produits dépourvus de garanties sont ainsi mis sur le marché puis modifiés de manière incrémentale en fonction des retours des utilisateurs, qui jouent alors le rôle de testeurs et s'exposent à un certain nombre de failles. On ne saurait imposer à une jeune *start-up* d'acquérir une certification témoignant d'un niveau de protection très élevé, parce qu'elle n'en aurait pas les moyens. En revanche, à partir d'un certain chiffre d'affaires, il conviendrait de renforcer les obligations de cybersécurité qui conditionnent la mise à disposition de logiciels au public.

Du côté des utilisateurs de logiciels, il a été imposé aux entreprises de présenter, dans leur bilan annuel, une déclaration de responsabilité sociale d'entreprise (RSE). De la même manière, pourquoi n'existerait-il pas une obligation de déclaration de politique de cybersécurité ? Comment les dirigeants d'entreprise pourraient-ils prendre en compte le risque de cybersécurité sans pression réglementaire de la part du législateur ?

Une troisième réponse est à chercher du côté de la formation des populations, dans un souci d'hygiène numérique. Le Gouvernement a mis en place, depuis quelques années, le service national universel (SNU), qui s'adresse à une population nativement numérique mais n'ayant jamais été éduquée à l'hygiène numérique. Pourquoi n'inclurait-on pas, dans le cadre du SNU, un module de formation à l'hygiène numérique, de sorte que cette nouvelle génération soit également sensibilisée à la cybersécurité ?

M. Julien Nocetti. Je partage tout à fait l'avis d'Olivier Kempf concernant les responsabilités incombant à nos éditeurs de logiciels, notamment pour faire part aux utilisateurs des failles de sécurité dont ils ont connaissance. Cela étant, aux États-Unis, un jeu constant du chat et de la souris a lieu entre les services et les failles inondant le marché noir.

Je distinguerai deux niveaux d'action. Au niveau macro, il est possible d'articuler des sanctions économiques et des inculpations de pirates informatiques, qui peuvent même donner lieu à des retournements de hackers acceptant de collaborer avec les pouvoirs publics pour renforcer notre résilience face aux cyberagressions. Ce cas de figure s'est produit récemment aux États-Unis. Cette démarche s'accompagne toutefois de risques d'escalade susceptibles de se retourner contre celui qui en est à l'origine : ces risques représentent une source aigüe d'inquiétude et de réflexion pour la France et l'Union européenne. Il serait judicieux d'élaborer une grammaire commune aux différents États en matière de cyberconflictualité. À la différence du domaine nucléaire, le domaine numérique irrigue toutes les activités humaines : la coordination entre acteurs devrait donc être constamment entretenue pour nous prémunir d'une crise systémique. Différentes propositions ont déjà été soumises par certaines parties prenantes, sans succès. Cette grammaire commune mettra certainement des années à se concrétiser, sachant que les puissances ne sont pas toujours d'accord sur ce que recouvrent les notions de cyberespace ou de cyberattaque.

Au niveau micro, un travail de longue haleine et très coûteux me semble indispensable pour résorber le risque cyber : ce travail, qui doit débuter dès le plus jeune âge, passe par la formation initiale et continue. À l'échelle mondiale, 3,5 millions d'experts en cybersécurité font aujourd'hui défaut, ce qui témoigne de l'urgence du besoin en matière de formation et de recrutement. La semaine dernière, lors du forum international sur la cybersécurité, la ministre des armées soulignait que la France forme un grand nombre d'experts techniques et d'ingénieurs de qualité. Cependant, les besoins en matière de cybersécurité dépassent de beaucoup les seules formations techniques : nous avons besoin de linguistes, de juristes, de philosophes, de sociologues, de managers formés à ces enjeux spécifiques. Il existe ainsi un besoin majeur d'hybridation des profils et des compétences.

M. Jean Lassalle. Vous nous avez présenté un monde chaotique dans lequel nous ne savons plus à qui nous fier ou contre qui nous défendre. D'ailleurs, les derniers évènements – la crise des sous-marins – tendent à le démontrer. Dans ce contexte, je me demande si nous n'avons pas fait preuve de naïveté en accordant autant de libertés à des sociétés vitales pour la France. Aurait-on laissé Alstom se jeter dans les bras de Siemens comme nous l'avons laissé se jeter dans les bras de General Electric ? Il est vrai qu'un effort très important est consenti depuis plusieurs années pour redonner à notre pays les moyens de son indépendance et de sa sécurité, mais n'avons-nous pas commis des fautes lourdes que nous risquons de payer ?

M. Olivier Kempf. Il n'est sans doute pas anodin que notre réunion se tienne une semaine après la mésaventure à laquelle vous faites référence. En tant que citoyen dépourvu d'expertise en matière industrielle, j'incline à considérer que les pouvoirs publics ont manqué d'inspiration dans l'affaire Alstom.

Devons-nous conclure de ces expériences qu'il nous faut mettre en œuvre une politique industrielle pour le secteur cyber ? C'est probablement le cas, mais à condition de faire preuve de doigté. En tant que consultant, j'accompagne une *start-up* travaillant dans le domaine de la confiance numérique. Avec cette PME, dont le secteur français de la défense est un client important, nous nous efforçons depuis un an d'organiser une levée de fonds. Or plus de 60 % des investisseurs que nous avons rencontrés se sont détournés de cette PME dès qu'ils ont su que nous travaillions dans le secteur de la défense. Nous payons ici, d'une certaine façon, les conséquences du refus de la cession de Photonis. Cette entreprise active dans le domaine de la cybersécurité avait suscité l'intérêt d'un acheteur américain. L'État s'était alors opposé à la vente en raison du caractère stratégique de cette entreprise. Si cette décision peut sembler compréhensible compte tenu des risques associés à une trop grande dépendance à l'étranger en matière de défense, elle a également conduit à un gel partiel des investissements, dont peuvent pâtir les acteurs français de la cybersécurité. En effet, ces investissements sont en quelque sorte l'engrais nécessaire à la croissance de notre industrie de la cybersécurité. Nous pouvons donc mettre en œuvre une politique industrielle pour promouvoir ce secteur, mais devons être conscients des conséquences de décisions trop tranchées.

La réunion se termine à dix-sept heures trente.

Membres présents ou excusés

Mission d'information sur la résilience nationale

Présents. - M. Alexandre Freschi, M. Thomas Gassilloud, M. Jean Lassalle, Mme Sereine Mauborgne, M. Buon Tan