ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

– Audition, ouverte à la presse, de M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie..... 2

Mardi
8 juin 2021
Séance de 11 heures 5

Compte rendu n° 83

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, rapporteur

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie

Présidence de M. Philippe Latombe, président et rapporteur

La séance est ouverte à onze heures cinq

M. Philippe Latombe, président et rapporteur. Nous avons l'honneur d'auditionner ce matin M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie.

Depuis près d'un an, notre mission d'information poursuit ses travaux sur les principaux enjeux de la souveraineté numérique. Parmi les thèmes que nous avons successivement abordés figure évidemment la cybersécurité, qu'il s'agisse de la nature et du niveau de la menace ainsi que de la réponse à y apporter.

M. le ministre, votre carrière et vos responsabilités ministérielles témoignent de votre exceptionnelle expertise dans ce domaine. C'est la raison pour laquelle nous attachons un grand prix à pouvoir vous entendre et échanger avec vous aujourd'hui.

En guise de propos liminaire, j'aborderai trois sujets.

D'abord, pourriez-vous nous partager votre conception de la souveraineté numérique ? Il s'agit d'une question rituelle que j'adresse à chaque personne auditionnée, et qui procède de la grande diversité de définitions qui peuvent être associées à cette notion. Comment appréhendez-vous donc ce concept et quelle peut être sa traduction concrète en termes de politiques publiques ?

Par ailleurs, nous souhaiterions connaître votre appréciation de la menace cyber et de ses différentes formes. Quel est l'état de la coopération en matière de cyberdéfense, qu'il s'agisse de coopérations bilatérales ou de la coopération au sein des instances de l'Union européenne ou de l'Organisation du traité de l'Atlantique nord (OTAN) ?

Enfin, comment jugez-vous le niveau de sensibilisation de la population ? Comment agissez-vous pour diffuser une culture de la protection contre le risque cyber au sein des acteurs publics ou privés ?

M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie. Merci beaucoup pour ces propos liminaires sympathiques. C'est un grand privilège d'être présent parmi vous au sein de l'Assemblée nationale et de vous faire part de notre point de vue sur la thématique de la cybersécurité. Nous venons récemment d'assister à une conférence dédiée à ce sujet, et je suis convaincu que vos travaux pourront bénéficier des différents points de vue exprimés par les autres pays de l'Union européenne.

Je commencerai par rappeler quelques définitions afin de répondre à votre première question relative à notre conception de la souveraineté numérique. De notre point de vue, trois éléments sont à prendre en compte pour répondre clairement à cette interrogation.

D'abord, quels sont les enjeux et de quoi parlons-nous ? Ici, le plus important est de bien comprendre les technologies dans le contexte de l'économie, de la concurrence, de la politique, mais aussi et surtout de la sécurité nationale. En effet, l'accès aux nouvelles technologies façonnera notre avenir et déterminera non seulement les avantages en termes technologiques, mais également le pouvoir économique et politique, ainsi que les structures de puissance au niveau mondial. Ce premier élément permet déjà de répondre partiellement à cette question relative à la souveraineté numérique.

Ensuite, quels sont les acteurs principaux ? Ici, il est essentiel d'identifier clairement les interactions entre les différents acteurs impliqués, notamment au niveau européen. Aujourd'hui, la Chine est clairement le premier acteur et la première puissance remettant en question le *statu quo* et les structures de puissance et de pouvoir. C'est vrai dans le domaine technologique, mais également de manière plus générale, puisque la Chine et l'Occident se font concurrence jusque dans leurs systèmes politico-économiques. Pour le sujet qui nous intéresse aujourd'hui, nous devons évoquer la technosphère chinoise, qui se développe de manière très active, ainsi que la technosphère occidentale, à laquelle nous appartenons en tant qu'Européens.

J'en profite d'ailleurs pour expliquer ce que j'entends par Occident ou monde démocratique, même s'il est sans doute plus risqué de m'exprimer à ce sujet devant l'Assemblée nationale que dans le cadre d'une conférence moins formelle. Lorsque je fais référence à l'Occident, je pense bien entendu et avant tout aux États-Unis. La Chine et les États-Unis sont deux pôles de compétition technologique. De mon point de vue, l'Union européenne n'a d'autres choix que de travailler étroitement avec les Américains. Des voix s'élèvent parfois pour promouvoir une relation triangulaire entre les États-Unis, l'Europe et la Chine, mais cette stratégie me paraît plutôt risquée. La coopération avec les Américains paraît au contraire la seule option viable pour que l'Europe soit considérée comme un acteur crédible capable de peser globalement. En tout état de cause, le Parlement est probablement l'endroit idoine pour discuter de la manière dont nous pourrions garantir cette coopération entre Américains et Européens en matière de technologies. Dans cette perspective, l'initiative visant à instituer un conseil du commerce et de la technologie entre Européens et Américains – et qui est au cœur des préparatifs du prochain sommet de l'OTAN – semble particulièrement pertinente. Les détails de sa mise en œuvre restent encore à régler, mais le message politique envoyé par la création de cette instance me semble tout à fait clair et très important.

Enfin, nous devons nécessairement nous interroger sur la manière de procéder pour sécuriser notre accès aux technologies et préserver le *statu quo*. Plusieurs éléments sont à prendre en compte. En premier lieu, il est primordial de faire évoluer nos mentalités, et c'est sans doute le message le plus important que je m'efforce de promouvoir. La Chine a jusqu'ici fortement tiré parti de sa coopération étroite avec les États-Unis, et nous devons nous en accommoder. En revanche, je suis convaincu que davantage de coopération avec Pékin ne peut qu'être contreproductif pour l'Union européenne. Il est donc crucial que ce changement d'état d'esprit survienne dans les plus brefs délais.

Deuxièmement, nous devons avoir conscience de la dépendance de nos chaînes d'approvisionnement. Dans différents secteurs, et pas uniquement dans le domaine technologique, nos chaînes d'approvisionnement sont extrêmement dépendantes de la Chine, ce qui est facteur de risques économiques et sécuritaires. D'ailleurs, en matière de sécurité, plusieurs aspects sont à prendre en compte, notamment en termes de sécurité nationale. Lorsque l'on analyse l'environnement légal et juridique en Chine, on constate que les entreprises technologiques sont contraintes de coopérer avec le régime communiste. En parallèle, un certain nombre d'activités malveillantes ont pu être clairement imputées à la Chine, comme le vol d'adresses IP ou diverses opérations d'espionnage. La volonté de nuire est donc bien réelle. Ainsi, à mesure que notre dépendance vis-à-vis des technologies s'accroîtra, les cibles potentielles d'attaques seront de plus en plus nombreuses.

Nous devons également discuter des menaces très concrètes de cybersécurité auxquelles nous sommes exposés. À cet égard, je me permettrai d'évoquer plusieurs rapports et analyses de sécurité produits par notre centre national de cybersécurité. Je pourrai d'ailleurs vous en laisser quelques exemplaires si vous souhaitez en apprendre davantage. L'année

dernière, nos experts ont conduit une analyse de sécurité sur les caméras fabriquées en Chine. Cette année, ils publieront un autre rapport sur les téléphones fabriqués en Chine. Ces équipements sont source de multiples menaces en termes de cybersécurité. Il est par exemple possible d'intercepter le contenu des caméras, mais aussi de capter, utiliser et diffuser des informations sensibles stockées dans les téléphones, à partir de messages cryptés et d'applications intégrées dans les terminaux téléphoniques. Ces problématiques de cybersécurité associées et intégrées aux technologies sont donc parfaitement identifiées.

Au-delà du changement de mentalité nécessaire pour sécuriser l'accès aux technologies, nous devons également protéger les infrastructures critiques. Nous avons multiplié les échanges autour de la 5G et de la manière de garantir l'implication de fabrications et de fournisseurs de confiance dans la construction de nos réseaux. En Lituanie, le Parlement a récemment adopté une loi sur les communications électroniques, qui introduit des critères très précis pour identifier ces fabricants de confiance, que nous définissons comme des entreprises provenant des États membres de l'OTAN, de l'Union européenne ou de l'Organisation de coopération et de développement économique (OCDE). Ce genre d'initiative mériterait d'être reproduit dans d'autres domaines critiques, par exemple dans le secteur de l'énergie, marqué par une forte dépendance à l'égard des produits chinois pour ce qui relève de l'énergie solaire, mais aussi dans le secteur des transports et des villes intelligentes. À l'avenir, nos vies seront extrêmement dépendantes de ces technologies. Il est donc primordial de protéger ces infrastructures.

Pour en revenir à l'exemple lituanien, j'évoquerai deux manières de protéger ces infrastructures critiques. D'abord, nous avons mis en place un solide mécanisme de sélection dans le cas des investissements et des marchés publics. Néanmoins, dans la mesure où cet outil s'avère insuffisant pour protéger efficacement nos infrastructures, nous avons commencé à travailler sur une législation dédiée. Tout comme pour la 5G, nous introduirons un critère de sécurité nationale dans l'ensemble des marchés publics de construction des infrastructures critiques, qui seront réservés non seulement aux entreprises des pays membres de l'OTAN, de l'Union européenne et de l'OCDE, mais plus largement aux entreprises des pays partageant nos valeurs et principes démocratiques, avec qui nous collaborerons pour construire ces infrastructures.

Enfin, pour garantir cette protection et cet accès aux technologies, il me paraît essentiel de raccourcir, d'occidentaliser et d'européaniser nos chaînes d'approvisionnement, afin de nous prémunir des risques que nous venons d'évoquer.

Sur le plan politique, nous savons que l'Europe investira de manière significative et collective dans la transformation numérique et dans la transition énergétique. Logiquement, ces fonds devront naturellement bénéficier aux entreprises européennes. Cela dit, il est encore plus primordial que la Chine et les entreprises chinoises n'en bénéficient pas, étant entendu qu'elles en sont aujourd'hui bénéficiaires. Le changement de mentalités que nous appelons de nos vœux doit donc parallèlement s'accompagner de nouveaux paradigmes politiques.

Comme vous l'avez compris au travers de cette réponse relativement longue à votre question initiale, notre conception de la souveraineté numérique repose avant tout sur le primat de la coopération transatlantique. Nous privilégions les alliances technologiques occidentales, et non la souveraineté technologique de l'Europe.

Votre seconde question portait sur la coopération en matière de cyberdéfense. Il s'agit également d'un sujet extrêmement vaste, notamment si on pense à la coopération européenne, qui vous intéresse plus particulièrement. En l'occurrence, la Lituanie est l'un des pays les plus ouverts à la coopération internationale en matière de cybersécurité. Dans ce domaine, j'évoquerai une initiative concrète que nous avons promue depuis près de deux ans.

En tant que pays européens, nous avons tous pris l'habitude d'échanger des informations de cybersécurité avec l'Union européenne et avons constitué des réseaux dédiés. Dans le même temps, de nombreux pays ont tendance à vouloir apporter des réponses nationales en matière de gestion des incidents de cybersécurité. Il n'est ainsi pas rare d'entendre des dirigeants français affirmer que ce sujet relève de prérogatives nationales. Pour notre part, nous considérons nécessaire de dépasser cette approche. Les investissements dans les capacités nationales sont évidemment nécessaires, mais cette stratégie plutôt facile à envisager pour les grands pays s'avère difficile à mettre en œuvre pour les petits États, dont les capacités nationales ne sont pas suffisantes pour faire face aux risques de cybersécurité.

Dans cette logique, nous avons piloté la création d'équipes d'intervention rapide en matière de cybersécurité (*Cyber Rapid Response Teams)* au niveau européen. Dans le format de l'Union européenne, la mise en place d'équipes opérationnelles à l'échelle communautaire s'avère toujours difficile et sensible. Malgré tout, nous sommes parvenus à trouver un compromis avec un certain nombre d'États membres à même de prendre des décisions, avec qui nous avons élaboré des capacités de réponse utilisables dans différents scénarios. Si nous sommes évidemment prêts à appuyer les institutions communautaires et les pays partenaires contribuant à cette initiative, nous sommes également disposés à assister d'autres États membres de l'Union européenne qui n'y sont pas associés.

Les deux dernières années ont été marquées par de véritables avancées pour ces équipes. Nous avons récemment conduit un exercice de déploiement en différents endroits pour aider à la résolution d'incidents de cybersécurité affectant plusieurs ambassades. En outre, et malgré le contexte pandémique Covid-19, nous avons élaboré des procédures logistiques permettant à ces équipes de gérer efficacement des incidents de cybersécurité. Enfin, nous avons mené plusieurs exercices de certification qui nous permettront de mettre en place des capacités d'intervention pleinement opérationnelles. En résumé, retenez que nous sommes parvenus à constituer une équipe multinationale de six États membres, qui peut être utilisée et déployée dans différents scénarios.

Bien entendu, d'autres initiatives de cyberdéfense reposent sur la coopération internationale. Néanmoins, l'initiative précitée est un projet phare et un projet européen, qui trouve son origine dans le dispositif de coopération structurée permanente (*Permanent Structured Cooperation, PESCO)* cadrant la coopération des États membres en matière de sécurité et de défense. Il s'avère que nous avons utilisé cet outil l'an dernier, en amont de nos élections parlementaires, afin de mettre à l'épreuve la résilience de nos réseaux. Comme me l'ont confirmé mes interlocuteurs français, la sécurité des élections est également un enjeu majeur dans votre pays, notamment en perspective de l'élection présidentielle de 2022. Nous sommes donc convenus d'approfondir nos discussions et de renforcer la coopération franco-lituanienne sur le sujet, avec l'objectif de sécuriser les processus électoraux, dans lesquels les questions de cybersécurité – mais aussi de désinformation – sont de plus en plus prégnantes.

J'en arrive à votre dernière question, qui est certainement la plus complexe à traiter. Quoi que l'on mette en œuvre, les menaces de cybersécurité sont une réalité avec laquelle nous devrons composer, puisqu'elles ne disparaîtront pas. À ce titre, je pense que le facteur humain et la sensibilisation sont des enjeux critiques en matière de cybersécurité. Il ne s'agit pas seulement d'investir dans les technologies et de protéger les infrastructures. Tout ceci ne sera d'aucune utilité si le grand public et les citoyens ne sont pas sensibilisés, puisqu'ils constitueront alors un maillon faible.

Dans cette perspective, nous avons récemment présenté notre rapport annuel sur le panorama des menaces de cybersécurité en Lituanie, en sensibilisant différents groupes et communautés – mais aussi la population générale – aux cybermenaces les plus actuelles. La

publicité et la visibilité offertes par ce rapport nous permettent de promouvoir et de défendre nos messages. En guise de conclusion, ce rapport montre que les incidents de cybersécurité doivent être considérés comme une menace pérenne. Ceux-ci ont progressé de 25 % par rapport à l'an dernier, en lien avec l'utilisation accrue des infrastructures numériques dans le contexte de Covid-19 et de confinement. Nous avons également observé une corrélation avec l'actualité politique, et notamment avec nos dernières élections législatives, durant lesquelles nous avons connu un pic d'incidents de cybersécurité. À cet égard, il est toujours intéressant d'observer le pourcentage d'incidents ciblant les institutions étatiques, les secteurs critiques et la population générale. Selon nos analyses, 10 % des incidents enregistrés ciblaient les institutions étatiques et les secteurs critiques. Par ailleurs, lorsque l'on cherche à savoir qui se cache derrière ces incidents, la réponse est très claire dans notre cas : il s'agit de la Russie. L'État russe sponsorise les cybermenaces, ce qui constitue un véritable enjeu. La Chine se veut également de plus en plus influente en Lituanie et dans la Baltique, et nous nous efforçons désormais de mettre fin à cette dépendance technologique de longue date et de nous prémunir des activités malveillantes soutenues par Pékin.

M. Philippe Latombe, rapporteur. Vous avez souligné que la Chine constituait la principale menace que vous appréhendiez. Pensez-vous que tous les États européens partagent la même sensibilité et la même vision de la menace que représente la Chine ? À l'inverse, pensez-vous qu'il existerait une forme de tropisme pour certains pays qui ne percevraient pas pareillement la menace chinoise ?

Par ailleurs, vous avez évoqué le rôle de la plaque russe en matière de cybercriminalité, du moins en matière de cyberattaques. Existe-t-il donc, d'après vous, un risque géopolitique technologique avec la Russie ?

M. Margiris Abukevicius. C'est justement pour répondre à ce type de questions que nous sommes ravis de partager nos perspectives avec les autres pays et d'enrichir le débat national. De notre point de vue, la menace chinoise en Europe n'est pas encore bien comprise. En Lituanie même, la perception de la Chine en tant que menace est relativement récente. Il y a quelques années, notre présidente se rendait en Chine avec une délégation de chefs d'entreprise et d'industriels à la recherche d'opportunités commerciales pour notre pays. Désormais, notre perception a évolué en sens contraire. Comme vous l'avez probablement entendu, nous avons officiellement quitté le format 17+1. Nous commençons à appréhender la Chine au travers du prisme sécuritaire, alors même que de nombreux pays européens continuent de privilégier un équilibre entre opportunités économiques et sécurité. Avec notre nouveau gouvernement entré en fonction il y a six mois, nous avons pris la décision tout à fait consciente d'appréhender notre coopération avec la Chine par le prisme de la sécurité, incluant les volets de cybersécurité et de dépendance technologique. Il me semble que c'est un défi que nous devons relever dans toute l'Europe. Pour les Américains, qui comprennent parfaitement les défis de long terme avec la Chine, la stratégie est relativement claire. En Europe, nous accusons un certain retard. Sitôt que nous aurons réellement compris la nature de la menace chinoise, nous façonnerons nos politiques en conséquence et serons beaucoup mieux préparés pour relever ces différents challenges.

Vous m'interrogez ensuite sur la Russie. S'il peut être intéressant d'évoquer le cas russe dans un échange sur la souveraineté technologique, force est de constater que la Russie n'est qu'un acteur marginal dans ce débat. Qu'il s'agisse de souveraineté technologique ou de dépendance aux technologies, nous ne considérons pas la Russie comme un acteur de premier plan, même si les Russes ont choisi de travailler avec la Chine dans ce domaine. Le fait est que la menace russe est parfaitement comprise – et depuis très longtemps – en Lituanie. Personne n'achète de technologies russes pour l'équipement des infrastructures critiques. À l'inverse, la Chine équipe toujours nos infrastructures, et nous devons nécessairement faire

évoluer nos mentalités. Cela dit, la Russie joue bien un rôle majeur en matière d'activités cyber malveillantes et représente une réelle menace pour la Lituanie.

M. Philippe Latombe, rapporteur. Je reviendrai brièvement sur le sujet de la Russie pour compléter notre échange. Au-delà de l'activité cybercriminelle que vous venez d'évoquer, vous avez souligné que la notion de souveraineté numérique devait également s'entendre au sens des *fake news* et de la capacité à diffuser de fausses informations pour influer sur les scrutins, comme vous avez pu l'expérimenter lors de vos dernières élections législatives. Ce sujet fut également prégnant lors des élections présidentielles américaines de 2016 ayant porté Donald Trump au pouvoir. D'après vous, comment pouvons-nous concilier souveraineté numérique et vérification des informations ? Estimez-vous que l'Europe se donne suffisamment les moyens de travailler sur le sujet pour éviter que nos sociétés démocratiques soient influencées, en période électorale, par les *fake news* et le complotisme ?

M. Margiris Abukevicius. Selon nos analyses, les menaces de cybersécurité associées aux campagnes d'information ou de désinformation sont particulièrement prégnantes et de plus en plus récurrentes. Du point de vue de l'influence sur les processus électoraux, ces menaces sont aujourd'hui le premier risque à prendre en compte. De nos jours, de nombreux pays sont fortement dépendants des technologies pour l'organisation de leur processus électoral. Grâce à la technologie, il est désormais possible d'influencer ce processus. En Lituanie, la technologie est naturellement intégrée à notre processus électoral, mais elle ne remplit pas un rôle critique. Nous devons donc nous assurer que tout fonctionne bien et ne pas donner à nos ennemis l'occasion de manipuler nos élections.

Dans cette perspective, la diffusion de fausses informations dans un contexte électoral constitue un moyen d'influence de premier plan. Il s'agit d'un processus de long terme, auquel nos adversaires se préparent à l'approche de chaque scrutin. Ces stratégies peuvent sinon changer les résultats d'une élection, du moins changer l'attitude d'un gouvernement. En tout état de cause, la désinformation et l'orientation de l'opinion s'inscrivent toutes deux dans une logique de long terme.

À cet égard, je citerai le rapport de la société de sécurité FireEye sur la campagne de désinformation menée par la Russie, qui couvre une période de cinq ans. Dans cette campagne intitulée *Ghostwriter*, une trentaine d'actions malveillantes de désinformation ont été relevées dans plusieurs pays européens. Une vingtaine de cas ont été détectés en Lituanie, mais d'autres pays – Pays baltes, Pologne, Allemagne – ont également été impactés. Du point de vue narratif, le contenu de cette campagne de désinformation était parfaitement clair : des messages contre l'Union européenne, contre l'OTAN et contre la présence militaire internationale dans la région. Par ailleurs, ces messages tentaient d'exploiter un certain nombre de fractures sociales caractérisant les sociétés concernées. Dans la plupart des cas, la technologie cyber a été utilisée en tant que moyen pour compromettre différentes plateformes médiatiques qui ont diffusé de fausses informations. Dans d'autres cas, la technologie cyber a été utilisée en sus de la désinformation en préparation de futures cyberattaques.

En tout état de cause, les actions malveillantes de désinformation sont désormais parties intégrantes du processus électoral. Nous devons donc y prêter une grande attention et favoriser le partage de bonnes pratiques et d'expériences.

M. Philippe Latombe, rapporteur. Dans votre propos liminaire, vous mentionniez l'existence d'une *task force* spécialisée en cybersécurité constituée avec d'autres pays. Si j'ai bien compris, cette équipe a vocation à s'agrandir pour fédérer davantage de participants. D'après vous, quelle taille optimale devrait atteindre cette équipe pour collecter et partager un maximum d'informations sans perdre en souplesse de fonctionnement ? Par ailleurs, à qui cette équipe doit-elle s'adresser ? Doit-elle nécessairement cibler le secteur

public et les institutions de l'Union européenne et des États membres ? Peut-elle éventuellement s'adresser aux entreprises du secteur privé, y compris aux plus petites ? Comment envisagez-vous le déploiement futur de cette équipe ?

M. Margiris Abukevicius. À ce stade, six États membres participent à cette initiative : la Lituanie, la Pologne, les Pays-Bas, la Roumanie, l'Estonie et la Croatie. D'autres pays ont quant à eux désigné des observateurs : s'ils ne participent pas activement à nos travaux et n'envoient pas d'experts, ces observateurs suivent attentivement nos débats et nos réflexions. La France figure d'ailleurs parmi ces pays observateurs avec qui nous partageons nos réflexions. En termes de dimensionnement, l'équipe elle-même n'est guère étoffée, puisqu'elle ne compte qu'une dizaine de membres, à savoir un représentant de chaque État membre et plusieurs experts. La direction opérationnelle du groupe est successivement assurée par chacun de ses membres, dans une direction annuelle tournante. Nous en sommes aujourd'hui à la deuxième mandature dirigée par la Pologne, sachant que la première était dirigée par la Lituanie. Nous ne chercherons pas à agrandir ce groupe à d'autres pays, puisque nous disposons précisément de la taille idoine pour fournir des réponses rapides dans le domaine de la cybersécurité. En revanche, si d'autres pays souhaitent nous rejoindre, nous pourrions créer plusieurs équipes distinctes, ce qui constitue un avantage non négligeable.

Sur le fond, nous nous interrogerons régulièrement sur la manière d'utiliser au mieux cet outil. Nous travaillons bien entendu avec les institutions européennes, non seulement au niveau politique, mais aussi de manière très concrète avec le personnel militaire afin de soutenir les opérations extérieures de l'Union européenne. Si nous disposions de plusieurs équipes, nous pourrions certainement en dédier certaines au volet militaire et d'autres au volet civil de la cybersécurité.

Nos partenaires en Europe sont évidemment les institutions communautaires et les États membres. Néanmoins, l'enjeu crucial demeure celui de notre relation avec les autres processus de l'Union européenne, qui n'est pas encore clairement établie. Bien entendu, notre équipe est encore très jeune, et nous tâchons de renforcer la visibilité de nos capacités. En tout état de cause, nous ambitionnons de nous intégrer pleinement aux mécanismes de réaction coordonnée de l'Union européenne face aux incidents de cybersécurité majeurs. La France et l'Italie jouent d'ailleurs un rôle moteur pour préparer l'Union européenne à ces incidents. Pour notre part, nous considérons notre équipe comme partie intégrante d'une boîte à outils plus large, vers laquelle l'Europe pourra naturellement se tourner pour avancer sur ce dossier.

Un autre élément majeur à prendre en compte est le fait que la Commission européenne a l'ambition politique de créer une unité commune de cybersécurité (*Joint Cyber Unit*). En l'occurrence, nous avons soutenu cette initiative depuis le début. Même si personne ne sait encore quelles seront précisément les attributions de cette unité commune de cybersécurité, il est certain qu'elle devrait faciliter l'échange d'informations relatives aux activités opérationnelles en matière de cybersécurité. Surtout, nous disposerons d'un bras armé et d'une équipe opérationnelle capable de soutenir les États membres. Dans ce contexte, nous devons éviter l'écueil des doublons et ne pas recréer, au niveau communautaire, des mécanismes déjà existants au niveau national. Au contraire, nous devons nous appuyer sur ce qui a déjà été mis en œuvre par les différents États membres. Avec un plus large soutien politique, nous pourrons certainement obtenir des financements pour développer certaines initiatives. En tout cas, plusieurs mécanismes fonctionnels existent déjà au niveau national.

Au-delà des institutions et des pouvoirs publics, nous travaillons également avec le secteur privé, et notamment avec de nombreux industriels français. Cette collaboration s'inscrit dans le cadre de l'initiative PESCO, mais également dans le cadre du Fonds européen de la défense, qui promeut la coopération industrielle à l'échelle communautaire. Nous avons

d'ailleurs soutenu une proposition qui consisterait, avec l'appui du Fonds européen de défense, à développer une boîte à outils pour les différentes équipes, sachant que chaque pays tend à développer ses propres outils, avec les problématiques d'interopérabilité que cela représente. Il s'agirait donc de standardiser la boîte à outils à disposition des équipes de réponse aux cyberattaques, qui pourrait alors être utilisée par notre groupe comme par d'autres équipes dédiées au sein de l'Europe. Nous avons de réels espoirs que notre consortium puisse mettre en œuvre ce projet, qui devrait normalement recevoir le feu vert de la Commission européenne dans le courant du mois. Pour information, ce consortium auquel est notamment associé le groupe français Thales est dirigé par la Lituanie et réunit d'autres entreprises de pays qui, s'ils ne sont pas associés aux équipes de réaction rapide, sont fortement intéressées par la coopération industrielle, comme l'entreprise italienne Leonardo. De fait, il s'agit d'un très bon exemple de coopération industrielle européenne dans le domaine de la cybersécurité et de la cyberdéfense.

M. Philippe Latombe, rapporteur. Dans votre propos liminaire, vous insistiez également sur l'importance accrue de la cybercriminalité, qui a pris de plus en plus d'ampleur en 2020, et qui prendra de plus en plus d'ampleur dans les années à venir. Vous avez justement rappelé que nous devions agir autant que faire se peut pour éviter que cette cybercriminalité n'affecte les réseaux critiques : 5G, transport, énergie. Dans ce contexte, comment pouvons-nous renforcer la robustesse de nos réseaux ? Savez-vous si d'autres pays ont suivi votre modèle en auditant leurs réseaux ? Quels sont aujourd'hui les risques dont l'Europe devrait se prémunir en priorité par rapport à ses réseaux critiques ?

Par ailleurs, comment devons-nous procéder pour endiguer les activités de cybercriminalité localisées à l'étranger, qu'elles proviennent de Russie, de Chine, de Corée du Nord ou d'ailleurs ? Démanteler une cellule ne revient-il pas à couper la tête d'une hydre qui repoussera nécessairement ailleurs ? Disposons-nous véritablement de moyens juridiques et technologiques pour endiguer définitivement ces menaces ? Avons-nous éventuellement besoin de nouveaux outils ?

M. Margiris Abukevicius. Il s'agit d'une question éminemment complexe, à laquelle nous pouvons répondre sous plusieurs angles. D'abord, comme je l'indiquais précédemment, il est impératif que nos réseaux soient construits et équipés par des fabricants de confiance si nous souhaitons véritablement réduire les risques. Par ailleurs, nous devons nous montrer intransigeants vis-à-vis des obligations des industriels en matière de conformité (*compliance*). En Lituanie, la législation impose aux industriels de respecter un certain nombre de critères en matière de cybersécurité. L'Europe s'oriente également dans cette direction grâce aux directives *Network and Information System Security (NIS)* 1 et 2. Les prérequis en matière de sécurité sont de plus en plus nombreux, mais il est toujours aussi difficile de s'assurer que les industriels s'y conforment totalement.

Plus largement, nous ne devons pas nous voiler la face et croire que nous serons en mesure de sécuriser totalement nos réseaux. Il est plus pertinent de se focaliser sur leur résilience en vue d'assurer la continuité des affaires. Nous ne pourrons jamais totalement endiguer les attaques de type rançongiciel (*ransomware*). En revanche, nous pouvons préparer nos entreprises à y faire face pour qu'elles puissent rapidement reprendre leurs activités après une attaque. Nous en revenons ici à la question des prérequis en matière de cybersécurité.

Enfin, l'échange d'informations est absolument critique. Plus nous coopérerons, plus nous disposerons d'informations et mieux nous serons préparés aux cyberattaques. J'en profite d'ailleurs pour mentionner une autre initiative internationale dirigée par la Lituanie, à savoir le centre régional de cyberdéfense. Trois autres pays y sont aujourd'hui associés : les États-Unis, la Géorgie et l'Ukraine. Un pilote a été lancé au mois de mai, avec des experts

américains, géorgiens et ukrainiens qui se sont déplacés jusqu'à Kaunas, deuxième ville de Lituanie, pour travailler, avec leurs homologues lituaniens, à la création d'une cellule multinationale de renseignements spécialisée en cybersécurité, qui centraliserait les différentes sources de renseignements en la matière au profit de différents pays. Bien qu'ayant une vocation régionale, ce centre implique des acteurs aussi différents que les Américains, les Géorgiens et les Ukrainiens, dans l'idée de répondre à la menace provenant de Russie. Plusieurs cyberattaques ont en effet été dirigées contre la Géorgie en 2008 et l'Ukraine en 2015, donnant ainsi l'occasion à notre ennemi de tester de nombreux outils tactiques dans cette région. Il s'agit donc d'amener ces pays particulièrement exposés à coopérer avec les pays de l'OTAN et de l'Union européenne pour mieux nous préparer à réagir à ces menaces.

M. Philippe Latombe, rapporteur. Nous sommes actuellement en phase de déconfinement et de reflux d'une pandémie contre laquelle nous disposons désormais d'un vaccin. Pensez-vous que cette période troublée de pandémie aura des effets bénéfiques sur la cybersécurité et sur la prise de conscience du risque cyber ? Les parties prenantes – les États, les entreprises et les citoyens – sont-elles désormais toutes convaincues que les avantages du numérique s'accompagnent d'un certain nombre de risques ? Y sont-elles plus sensibilisées ? Pensez-vous que cette évolution était nécessaire et qu'elle perdurera dans les années à venir ?

M. Margiris Abukevicius. Vous m'interrogez sur les liens entre la Covid-19, le confinement et les cybermenaces. En l'occurrence, notre rapport annuel sur les cybermenaces a mis en avant un pic significatif d'incidents de cybersécurité survenus durant le premier confinement, lorsque les populations utilisaient tous les outils de communication à disposition sans se préoccuper des risques de cybersécurité. Durant le deuxième confinement, les cyberattaques se sont poursuivies, mais à une plus petite échelle, étant entendu que nous y étions beaucoup mieux préparés suite à l'expérience du premier confinement.

En tout état de cause, le premier confinement a considérablement accéléré l'usage des différents outils et services numériques. Logiquement, nous continuerons de nous en servir à l'avenir, même si nous ignorons encore à quel rythme se propagera cet usage massif des technologies numériques. En revanche, nous savons que cette utilisation accrue de la technologie élargit le périmètre de la menace, accroît les possibilités d'influence et diminue l'efficacité des moyens de protection. De fait, dans notre agenda national, nous nous efforçons de concilier les impératifs de numérisation et de cybersécurité. Sans cybersécurité, nous ne serons pas en mesure de nous appuyer sur les technologies numériques.

Dans le contexte des nouvelles perspectives financières de l'Union européenne, nous savons que le plan de relance européen accorde une large place à la transformation numérique. Nous avons donc convenu qu'environ 10 % des investissements consacrés à cette transformation numérique seraient dédiés à la cybersécurité. Il s'agit d'un véritable changement, qui est évidemment bienvenu. Nous disposons en effet de nombreux systèmes d'information obsolètes, et nous passons notre temps à résoudre des incidents de cybersécurité affectant ces systèmes construits à une époque où personne ne se souciait de cette thématique. En tout état de cause, pour accompagner ce bond numérique, nous devons sérieusement penser aux impératifs de cybersécurité et intégrer cette dimension en amont de chaque projet.

M. Philippe Latombe, rapporteur. Plusieurs évolutions technologiques sont attendues dans les années à venir : Internet des objets ; voitures autonomes ou semi-autonomes ; avions presque exclusivement gérés par l'informatique ; automatisation et robotisation des procédés industriels ; etc. Quelles sont donc vos craintes ou vos perspectives en matière de cybersécurité ? Pensez-vous que ces évolutions contribueront à changer la manière dont les cybercriminels s'attaquent aux entreprises ou aux administrations ? Devons-

nous nous attendre à des évolutions technologiques telles que nous devrons modifier notre manière de répondre aux attaques ? Au contraire, conserverons-nous les mêmes modes de fonctionnement et devrons-nous y apporter les mêmes réponses qu'aujourd'hui ?

M. Margiris Abukevicius. Les cybercriminels et les acteurs malveillants sauront s'adapter aux nouvelles technologies et aux nouvelles réalités. Si nous nous appuyons sur des systèmes autonomes ou semi-autonomes, ils chercheront nécessairement à exploiter les failles de nos systèmes de défense, qui devront eux-mêmes s'adapter. De nos jours, la question n'est plus de savoir si cette évolution se concrétisera, mais de savoir quand celle-ci se concrétisera. L'avenir sera certainement marqué par une dépendance à l'égard des technologies, et les impératifs de sécurité devront être pris en considération dès la phase de conception des différents systèmes, dans une logique de *security by design*.

Sur un plan plus personnel, bien que plutôt jeune et n'ayant jamais utilisé un téléphone avec des boutons, je refuse obstinément de connecter mon réfrigérateur au Wi-Fi ou d'accéder à distance aux systèmes de contrôle de ma voiture. *In fine*, je me protège et prends des décisions en toute conscience pour éviter toute sur-dépendance vis-à-vis des technologies numériques. Quoi qu'il en soit, dans la mesure où la société dans son ensemble sera de plus en plus dépendante des technologies, la prise en compte et l'intégration des mesures de sécurité constitueront des enjeux essentiels du débat public de demain.

M. Philippe Latombe, rapporteur. En conclusion, souhaiteriez-vous transmettre un dernier message aux parlementaires français en ce qui concerne la cybersécurité ? Considérez-vous qu'il existe un sujet sur lequel nous devrions absolument nous pencher ?

M. Margiris Abukevicius. Je souhaiterais évidemment insister sur la coopération transatlantique en matière de technologies et de cybersécurité, que j'ai évoquée à plusieurs reprises dans mon intervention. Il est absolument critique d'aller au-delà du périmètre de l'Union européenne. Bien entendu, il est logique de promouvoir l'usage de produits européens pour préserver notre industrie. Néanmoins, il me paraît primordial d'élargir le périmètre de notre stratégie en matière de cybersécurité et de la concevoir dans l'alliance transatlantique. Dans d'autres domaines, les exemples de coopération entre les États-Unis et l'Europe ne manquent pas, notamment en matière de sécurité. En tout cas, une alliance technologique entre les États-Unis et l'Europe aurait nécessairement un impact mondial. Dans cette alliance, chaque pays devrait promouvoir sa propre industrie et bâtir des chaînes d'approvisionnement efficaces. Notre vision doit toutefois porter au-delà de l'Union européenne pour inclure une dimension transatlantique, sachant qu'une coopération dans le domaine des technologies permettra certainement de revivifier cette alliance. Voilà donc le message que je souhaiterais faire passer aux députés français.

M. Philippe Latombe, rapporteur. M. le ministre, je vous remercie de votre message, de vos réponses et d'avoir consacré du temps à cette audition. Nous ne manquerons pas de relayer votre plaidoyer en faveur d'une coopération accrue avec les États-Unis en matière de cybersécurité, de même que votre message de vigilance à l'égard de la Chine.

La séance s'achève à douze heures dix

Membres présents ou excusés

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

Réunion du mardi 8 juin à onze heures cinq

Présent. – M. Philippe Latombe

Excusés. – Mme Marietta Karamanli, MM. Jean-Michel Mis, Jean-Luc Warsmann