ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Mercredi
4 juillet 2018
Séance de 11 heures 30

Compte rendu n° 69

SESSION EXTRAORDINAIRE DE **2017-2018**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de M. Jean-Jacques Bridey, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures trente.

Mme Alexandra Valetta-Ardisson, rapporteure. M. le Président, chers collègues, demain, est-ce qu'une succession logique de 0 et de 1 au sein d'un code informatique binaire pourra provoquer autant de dégâts qu'un missile de croisière naval ou qu'un obus tiré par un canon Caesar, en rendant inutilisables des équipements, des matériels ou des infrastructures militaires ? Est-ce qu'un virus aux effets systémiques, par la désorganisation massive qu'il provoquera, pourra aboutir à la mort d'êtres humains, y compris des civils ? Comme le souligne la Revue stratégique de cyberdéfense publiée par le SGDSN, il est probable qu'une attaque informatique consistant en des actes de blocage ou de sabotage des systèmes informatiques aura, un jour, des conséquences létales.

Ce qui, hier encore, pouvait relever de la science-fiction apparaît dorénavant comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société.

L'intérêt et la compétence de notre commission pour le « sujet cyber » sont évidents et légitimes. Les fondements de notre système de cyberdéfense ont majoritairement été posés dans le cadre des différentes LPM adoptées depuis 2009. La LPM 2019-2025, qui devrait être promulguée dans une dizaine de jours, ne fait d'ailleurs pas exception : un chapitre spécifique y est ainsi consacré.

Avant d'entrer dans le vif du sujet, je formulerai deux remarques liminaires de « méthodologie ».

Tout d'abord, notre rapport ne prétend pas à l'exhaustivité, et ce pour plusieurs raisons. Premièrement, le cyber est par nature une réalité globale, qui touche pour ainsi dire tous les champs de l'activité sociale. Il dépasse donc le champ de compétence d'une seule commission.

Deuxièmement, c'est un domaine en perpétuelle évolution. Son analyse n'est donc pas et ne sera jamais achevée.

Troisièmement, la Revue stratégique de cyberdéfense a déjà dressé un panorama très complet de la question, et il était évidemment inutile de doublonner le travail déjà effectué dans ce cadre.

Enfin, il faut rester conscient du fait que les travaux menés dans ce domaine se heurtent rapidement à l'obstacle du secret de la défense nationale. En matière cyber comme en matière de renseignement par exemple, tout n'est pas dicible, encore moins publiable. Je vous laisse imaginer la situation lorsqu'un même service cumule compétences en matière de renseignement et en matière cyber… Si toutes nos questions n'ont pas pu trouver réponse du fait de ce nécessaire secret, nos interlocuteurs ont toujours fait preuve de la plus grande ouverture possible et permise pour éclairer nos travaux. Ils n'ont pas hésité à nous faire part d'éléments certes non couverts par le secret, mais néanmoins sensibles et nécessaires à la compréhension du sujet. Nous ne pouvons évidemment pas en faire état, mais nous tenons à souligner l'excellent état d'esprit de nos interlocuteurs, et à les en remercier.

La seconde précision méthodologique est que notre rapport n'a pas vocation à constituer le guide de référence du parfait cyber-attaquant ou du parfait cyber-défenseur. Nous ne sommes donc pas rentrés dans des considérations trop techniques, puisque telle n'est pas notre vocation et que tel n'est pas l'intérêt de ce travail.

Ce rapport étant fait au nom de la commission de la Défense nationale et des forces armées, nous nous sommes attachés plus particulièrement aux problématiques intéressant la défense. Mais pas exclusivement toutefois, puisque le cyber irrigue tous les domaines et brouille les frontières traditionnelles entre les États, entre les acteurs et entre les secteurs.

La « cyberguerre », au sens d'un conflit mené exclusivement dans le cyberespace avec l'emploi des seules armes cyber n'est sans doute pas une réalité opérationnelle. Du moins pas encore. Mais il n'y aura plus, demain, de conflit sans dimension cyber. Le cyberespace est un espace qui n'est ni en guerre ni en paix, mais en état de tension permanente. Un tel constat exige de ce fait une organisation et la mise en place de politiques et d'actions à la fois spécifiques et globales de la part des pouvoirs publics.

Nous n'allons pas abuser de votre patience avec de longs rappels sur l'organisation de la cyberdéfense en France, sur l'état de la menace ou sur les dernières cyberattaques massives qui ont eu lieu un peu partout dans le monde. Nous avons abordé ces sujets à l'occasion de l'examen de la LPM, et vous trouverez de longs développements consacrés à ces différents aspects dans le rapport écrit. Nous allons simplement revenir sur un certain nombre de points qui nous semblent importants, avant de vous présenter nos principales observations et recommandations.

Tout d'abord, de quoi parle-t-on lorsqu'on évoque la cyberdéfense ?

Le sujet étant assez technique, il semble nécessaire de définir quelques notions au préalable. Vous trouverez plusieurs définitions dans la version écrite du rapport. Dans le cadre de cette présentation, je n'en rappellerai que deux.

La cyberdéfense comprend l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels. Il ne faut pas la confondre, comme on le fait souvent, avec la cybersécurité. En résumé, celle-ci est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace et susceptibles de le compromettre.

M. Bastien Lachaud, rapporteur. J'en viens maintenant à la définition du cyberespace. Elle sera un peu plus longue. Cela peut sembler évident mais un tel rappel est important : le cyberespace est un milieu artificiel, créé par l'homme. Il ne s'agit pas d'un milieu naturel, comme les milieux traditionnels. C'est aussi un milieu abstrait et global, sans consistance physique. Il ne connaît ni limites ni réalités ou caractéristiques géographiques physiques. Il ne connaît pas non plus de frontières politiques ou juridiques qui permettraient, d'une part, d'en délimiter précisément les contours et, d'autre part, de le subdiviser pour en rattacher les différentes composantes à chaque État, ou à aucun d'entre eux.

Le cyberespace est également un espace mouvant qui est en recréation constante. Il n'existe pas de carte du cyberespace, de ses « continents » et de ses limites. De fait, le cyberespace et les conflits qui s'y déroulent sont à repenser en permanence.

En dépit de ces caractéristiques – ou grâce à elles –, le cyberespace constitue un nouveau théâtre d'opérations potentiel, au même titre cette fois que les espaces traditionnels. Des acteurs, étatiques ou non–étatiques, y agissent et l'utilisent pour atteindre des buts politiques, en exploitant toutes les possibilités offertes par ce nouveau milieu. De ce point de vue, le cyberespace ne diffère pas fondamentalement des quatre autres milieux. Et les actions qui y sont menées ne se distinguent pas, dans leur nature, des actions traditionnellement conduites, en particulier par les États : espionnage, sabotage, déstabilisation.

Enfin, le cyberespace est un espace global qui, en s'y superposant, et en les englobant, contient les espaces traditionnels.

Comment le cyberespace est-il structuré ? Comme le monde physique, il n'est pas homogène ; il se compose de trois couches distinctes qui font l'objet d'une régulation plus ou moins poussée.

On trouve d'abord la couche physique. En effet, même le cyberespace n'est pas totalement abstrait. Cette couche comprend globalement deux types de « matériels ». D'une part, l'ensemble des infrastructures qui permettent l'acheminement et l'échange des données au sein du cyberespace, y compris les lieux de stockage de l'information. Il s'agit des serveurs, des câbles sous-marins, ou encore des réseaux de fibre optique terrestre. On y trouve d'autre part les appareils terminaux que nous utilisons quotidiennement : ordinateurs, téléphones, tablettes numériques, objets connectés, systèmes électroniques, etc.

La couche physique du cyberespace peut être « territorialisée » juridiquement. S'agissant d'éléments physiquement situés sur des espaces donnés, ces différentes infrastructures et la couche qui les regroupe font l'objet d'une régulation, et sont soumises à différents niveaux de législations et de juridictions, tant nationales qu'internationales.

La couche physique et ses éléments peuvent être la cible d'actes malveillants, soit *via* le cyberespace, soit par des moyens tout à fait conventionnels et classiques : endommagement, altération, destruction, neutralisation, perturbation du fonctionnement, etc.

La deuxième couche du cyberespace est la couche logique. Elle comprend l'ensemble des programmes qui permettent d'accéder aux différents réseaux du cyberespace, de les exploiter, d'assurer le transport des données, etc. Il s'agit des différents protocoles, langages et autres logiciels mis en œuvre dans le cyberespace.

C'est cette couche qui constitue classiquement la cible des menaces cybernétiques, car elle est relativement facile d'accès. Par ailleurs, ses éléments présentent par nature des vulnérabilités. Il peut par exemple s'agir d'une erreur dans le code informatique d'un équipement, qui constitue alors une faille. À titre d'exemple, on estime qu'une erreur est présente en moyenne toutes les 1 000 lignes de code. Pour donner un ordre d'idée du nombre de failles potentielles – qui peuvent être d'importance et de gravité très diverses –, Google et l'ensemble des projets associés représenteraient deux milliards de lignes de code, Facebook plus de 60 millions, une FREMM plusieurs millions.

Dans la couche logique, le code constitue à la fois la vulnérabilité et le principal levier d'action, précisément pour exploiter les vulnérabilités adverses. L'attaquant est alors à la recherche de failles de sécurité susceptibles d'être exploitées. Les plus valorisées sont les failles dites *zero-day*. Il s'agit de vulnérabilités affectant un système, inconnues de leur

concepteur, qui n'ont jamais été identifiées et répertoriées, qui n'ont jamais fait l'objet d'une publication, et dont la communauté de la sécurité informatique n'a donc pas connaissance. Elles confèrent donc à leur « découvreur » un avantage tactique certain, du moins jusqu'à ce que, une fois dévoilées, des correctifs leur soient apportés.

Mme Alexandra Valetta-Ardisson, rapporteure. Troisième et dernière couche : la couche cognitive. Il s'agit de la couche du sens et du contenu visibles sur les divers sites et pages Internet, dans les systèmes de messagerie électronique ou sur les réseaux sociaux. Si les deux premières couches sont des couches techniques, la couche cognitive est celle de la valeur « sociale et intellectuelle », qui constitue le cœur du cyberespace. C'est une couche par essence ouverte et globale, impossible à réguler totalement compte tenu de son étendue et de sa nature. Sans même évoquer le *darkweb*, on estime ainsi qu'il existe plus d'1,8 milliard de sites Internet représentant plus de 4,5 milliards de pages. Chaque minute, 400 heures de vidéos sont téléchargées sur la plateforme YouTube, 216 millions de photos sont « aimées » sur Facebook et 350 000 tweets sont publiés sur Twitter.

L'étendue de cette couche emporte un grand nombre de vulnérabilités associées, chaque élément pouvant être exploité, transformé, détourné par un acteur malveillant. Nous en avons encore eu la preuve à l'occasion de grands rendez-vous démocratiques récents. Je pense aux cyberattaques subies par le *Democratic National Committee* lors de la campagne présidentielle américaine de 2016, ou à celles qui ont ciblé le site Internet du mouvement En Marche ! lors de la campagne présidentielle française de 2017.

C'est sur cette couche que se déploient l'information, mais également la désinformation, les activités de propagande ou encore les rumeurs et autres *fake news*. Si de telles réalités sont anciennes, la numérisation et l'interconnexion des sociétés permettent la production et la diffusion des contre-vérités à l'échelle industrielle.

Je souhaiterais maintenant présenter les spécificités du milieu cyber comme espace de conflit, du point de vue de la défense nationale.

Le cyberespace écrase les distances et le temps. Nous l'avons souligné : le cyberespace ne connaît pas de frontières. Il n'existe pas de cyberespace français dont la violation constituerait une atteinte. Aussi et pour reprendre un terme militaire : il n'y a pas de front dans le cyberespace, ou alors il s'agit d'un front global. De fait, l'espace cyber pousse à l'extrême la disjonction entre, d'une part, la présence physique d'un acteur et le lieu de déclenchement de son action et, d'autre part, les effets de cette action.

Inversement, une attaque ciblée *a priori* peut, du fait de l'interconnexion des différents acteurs, également toucher une « victime collatérale ». Tel fut le cas pour la société française Saint–Gobain, victime indirecte mais bien réelle de la cyberattaque NotPetya qui avait ciblé l'économie ukrainienne en 2017. Le groupe français a ainsi été touché par le biais d'une filiale située dans ce pays, laquelle utilisait un logiciel de comptabilité dont la mise à jour avait été piégée, et qui a servi de canal à la dissémination du virus.

Par ailleurs, le cyberespace offre une protection naturelle aux auteurs d'actes malveillants. Un attaquant situé dans un pays donné peut parfaitement déclencher son action à partir d'un équipement situé dans un pays tiers, voire effectuer de multiples « rebonds » afin de masquer la véritable origine de l'attaque. C'est l'une des difficultés à laquelle se heurtent les autorités et services chargés d'attribuer une cyberattaque. Nous y reviendrons.

En s'affranchissant de l'une des barrières les plus contraignantes qui soit – la distance, et donc le temps – l'attaquant dispose dans le milieu cyber, d'un avantage stratégique non négligeable : l'effet de surprise.

Le temps est un autre facteur classique déterminant dans les espaces traditionnels de conflits. Là encore, le cyberespace s'en distingue puisque la dimension temporelle devient secondaire. Une cyberattaque peut présenter un caractère foudroyant. En une seule commande, en un « clic » de souris, un attaquant peut obtenir de manière quasi instantanée l'effet recherché : corruption d'un système, défiguration, blocage, ou encore déni de service.

Toutefois, si la transmission des ordres informatiques se caractérise par sa rapidité extrême, l'action cybernétique peut également favoriser le temps long. Certaines formes de corruption de systèmes, notamment les bombes logiques, peuvent en réalité être présentes dans ces systèmes pendant une longue période avant d'être déclenchées ou de se déclencher de manière automatique.

Par ailleurs, les attaques informatiques nécessitent une phase de préparation parfois longue afin d'analyser la cible de la manière la plus fine possible. Après le déclenchement de l'attaque, les phases d'intrusion au sein d'un système puis d'exploitation de celui-ci peuvent également nécessiter du temps, surtout si l'architecture du système visé est complexe. À titre d'exemple, la cyberattaque qui a affecté TV5 Monde s'est déroulée sur près de trois mois, entre l'intrusion dans les réseaux de la chaîne et la production des effets de l'attaque.

Enfin, l'attaquant ne cherche pas systématiquement à conférer une publicité à son acte. Car l'efficacité de certaines atteintes repose au contraire sur le caractère indétectable de celles-ci. On pense notamment au vol de données.

Le cyberespace permet par ailleurs un certain nivellement des rapports de force. Cela tient d'abord à la relative facilité d'accès aux technologies cyber. Alors qu'il est assez malaisé de se procurer des armes « classiques », compte tenu de l'existence de régimes de régulation et d'interdiction, l'accès aux potentielles armes cyber est relativement ouvert. Par ailleurs, même « rustique », un programme malveillant répliqué des centaines de milliers de fois peut produire des conséquences massives. Soulignons enfin la disproportion entre la « taille » d'une arme cyber et ses effets : on estime ainsi que le virus Stuxnet, qui a affecté le fonctionnement de certains sites nucléaires iraniens en 2010, « pesait » entre 500 kilo-octets et 1 méga-octet selon les versions, soit l'équivalent d'une simple photographie numérique de qualité raisonnable.

En second lieu, ce nivellement est la conséquence d'une imbrication entre les milieux civil et militaire, qui brouille la ligne de partage traditionnelle des conflits. Dans le cyberespace, le rapport entre cibles civiles et militaires s'inverse puisque les premières représentent la « norme ». Elles sont, du reste, comparativement moins bien protégées que les secondes et constituent à cet égard des cibles de choix pour les attaquants. Or même ciblées sur des éléments exclusivement civils, des atteintes peuvent mettre en danger le fonctionnement normal d'une société, voire la survie de la Nation. Le cyberespace produit donc une confusion entre les sphères civiles et militaires, à rebours de la pensée stratégique traditionnelle et des régimes juridiques applicables aux conflits. En effet, ceux-ci reposent sur une distinction claire, même si elle n'est pas toujours respectée en pratique, entre ces deux champs.

M. Bastien Lachaud, rapporteur. Troisième spécificité : l'attribution d'une cyberattaque est très complexe. Pour faire usage de la force de manière légitime, adaptée et proportionnée à l'égard d'un agresseur, il convient de l'avoir préalablement identifié et d'être en mesure de lui imputer de manière certaine l'acte qui justifie l'action exercée en retour. Or dans le cyberespace, l'attribution s'avère particulièrement difficile, ce qui complique singulièrement les capacités de réponse à une cyberattaque. Plusieurs raisons l'expliquent :

– les actions malveillantes menées dans ce milieu font très rarement – voire jamais – l'objet d'une revendication. Par ailleurs, l'attaquant originel, s'il peut être identifié, n'est pas nécessairement le commanditaire de l'action ;

– on l'a dit, rares sont les attaques directes déclenchées à partir d'un point A pour affecter immédiatement et sans détour un point B. Les cyber–attaquants s'efforcent de faire « rebondir » leurs attaques de serveur en serveur et de pays en pays afin de « masquer leurs traces » ;

– au-delà des victimes expressément ciblées, une cyberattaque peut également affecter des victimes « collatérales », que l'attaquant ne cherchait pas spécifiquement à atteindre ;

– le cyberespace offre à ses acteurs un degré d'anonymat sans équivalent, et remonter la « chaîne d'anonymisation » représente un défi majeur. C'est d'autant plus vrai s'agissant des entités, groupes ou individus qui agissent non pas sur les réseaux ouverts, mais sur le *darkweb* ;

– les effets de certaines atteintes peuvent se déclencher longtemps après la pénétration effective d'un système.

Il convient toutefois de souligner un aspect essentiel. Au-delà des aspects purement techniques, la décision d'attribuer une cyberattaque relève, en dernière analyse, d'une appréciation et donc d'une décision de nature politique. Plutôt que sur des certitudes absolues et des preuves irréfutables, une telle décision s'appuie sur un niveau suffisamment bas d'incertitudes, sur un faisceau d'indices à la lumière desquels l'autorité politique prend la responsabilité d'attribuer un acte. Contrairement à d'autres pays – États-Unis ou Royaume-Uni, par exemple –, la France n'attribue jamais officiellement les cyberattaques qui pourraient la cibler.

Comme l'affirmait Napoléon de manière particulièrement imagée mais très pertinente : « *En guerre comme en amour, pour en finir, il faut se voir de près.* » Or, le cyberespace empêche précisément de voir distinctement son adversaire. L'anonymat n'y est pas absolu et toute action numérique peut finir par être tracée. Mais les délais nécessaires pour lever cet anonymat et obtenir la parfaite traçabilité d'une action peuvent s'avérer incompatibles avec la conduite d'une action de représailles.

Une conséquence majeure de cette difficulté d'attribution est de rendre partiellement inopérants les mécanismes de défense collective existants : article 51 de la Charte des Nations unies, article 5 du traité de l'Atlantique Nord, article 42-7 du traité sur l'Union européenne. Vous trouverez dans le rapport écrit des développements à ce sujet.

Nous ne reviendrons pas sur les mesures qui ont déjà été prises en matière de cyberdéfense ces dernières années. Là aussi, vous trouverez toutes les éléments nécessaires dans le rapport publié. Nous allons maintenant vous faire part de nos principales réflexions, que nous avons choisi de présenter autour d'une grande recommandation « de principe » et de six grands thèmes. Nous les exposons en toute modestie, compte tenu du caractère global et extrêmement mouvant de la question.

Notre recommandation de principe est l'élaboration d'une grande loi cyber, à l'image de la loi « informatique et libertés » de 1978 ou encore des lois « bioéthiques ». En effet, le caractère global de la question cyber justifie :

– d'une part, une analyse approfondie et complète du sujet à l'échelle de notre pays ;

– et, d'autre part, la mise en place d'un cadre global et adapté, au–delà des dispositions qui ont été élaborées jusqu'alors, et qui ne concernent qu'un nombre réduit d'acteurs très spécifiques, à l'image des opérateurs d'importance vitale (OIV).

Une telle loi permettrait d'établir, à l'échelle nationale, une cartographie précise des vulnérabilités et des besoins, d'évaluer les ressources financières, matérielles et techniques nécessaires, et de déterminer les politiques à mettre en œuvre, qu'il s'agisse de politique industrielle, de recherche, ou encore d'adaptation du cadre juridique.

Comme les lois « bioéthiques », cette loi « cyber » pourrait faire l'objet d'un suivi et de mises à jour régulières. Un comité consultatif national du cyber, non permanent, pourrait être créé. Il serait chargé des travaux préparatoires à la révision de la loi cyber. À l'issue du processus de révision, le suivi du texte pourrait être assuré par des structures existantes, comme l'ANSSI.

J'en viens maintenant à la première série de recommandations, qui visent à nous permettre de recouvrer notre souveraineté numérique. Certaines rejoignent les observations qu'ont pu faire nos collègues Becht et Gassilloud à l'occasion de leur rapport sur la numérisation des armées.

Nous pensons avant tout nécessaire de créer des espaces de stockage souverains qui permettraient de rapatrier et de stocker nos données sur des territoires sous juridiction nationale ou européenne. Car les données stockées à l'étranger ne bénéficient d'aucune garantie quant à leur sécurité. Par ailleurs, certains États prétendent à l'application extraterritoriale de leurs législations. C'est le cas du droit américain. Ainsi, des données stockées hors des États-Unis mais sur des serveurs appartenant à des sociétés américaines ne peuvent pas être considérées comme totalement sécurisées.

Il convient donc de développer des espaces de stockage à distance – en *cloud* –, ou des centres de stockage « en dur ». Nous sommes bien conscients que le *cloud* souverain ne constitue pas l'alpha et l'oméga de la sécurisation des données. Il reste toutefois un levier puissant à ne pas négliger, pour peu que l'on tire les leçons des échecs du passé dans ce domaine.

L'utilisation de ces solutions souveraines pourrait être rendue obligatoire pour certains acteurs : personnes publiques, OIV, entreprises de la BITD. Un travail préalable de classification des données, dont une partie seulement a vocation à être stockée dans un espace

souverain, devra impérativement être effectué en amont. Cette évaluation de la nature des données et du niveau de protection requis est le gage de l'efficacité et, en définitive, de la viabilité des solutions qui seront proposées.

Ces solutions souveraines seraient aussi ouvertes aux autres acteurs, qui pourraient se voir délivrer un certificat par l'ANSSI qui attesterait du degré de sécurisation de leurs données. Un tel certificat pourrait même constituer un critère de valorisation des offres dans le cadre de l'attribution des marchés publics, sous réserve du respect de la réglementation européenne applicable et du code des marchés publics.

Sans se fondre dans un *cloud* transnational, les solutions nationales adoptées par la France et d'autres pays de l'Union européenne devront ouvrir la voie à un second niveau de stockage souverain, à l'échelle européenne. Celui-ci assurera un haut degré de protection aux données éligibles, qu'il conviendra de définir.

Mme Alexandra Valetta-Ardisson, rapporteure. Au-delà de la question du stockage, il est également nécessaire de disposer d'une certaine maîtrise de l'ensemble de l'écosystème numérique. Cela passe notamment par l'existence de solutions techniques alternatives, nationales et européennes, dans le domaine des logiciels et des composants, y compris grand public : moteurs de recherche, systèmes d'exploitation, logiciels de bureautique. Car, à l'heure actuelle, ces secteurs restent dominés par des monopoles ou quasi-monopoles non-européens, qu'ils soient américains ou chinois.

De telles solutions permettraient de réduire notre exposition au risque numérique. En effet, certains logiciels et composants peuvent parfaitement être piégés « à la source », intentionnellement ou non, et constituer des *backdoors* – ou portes dérobées –, qui sont autant de vulnérabilités potentielles. Par ailleurs, ces outils participeraient au renforcement de la souveraineté industrielle européenne, voire nationale. À cet égard, à côté de « l'Europe du *cloud* », « l'Europe du logiciel » pourrait constituer un projet concret et fédérateur.

Deuxième thème : le renforcement de la résilience de l'ensemble des acteurs. Si certaines administrations sont particulièrement conscientes des enjeux et des risques, par nécessité comme par « culture », tel n'est pas forcément le cas de toutes. Or, un attaquant ciblera plus volontiers les maillons les plus faibles d'une chaîne si cela lui permet d'atteindre, par répercussion, les plus forts.

C'est pourquoi il semble indispensable :

– de durcir les dispositifs de prévention et de protection de l'ensemble des autorités publiques nationales ;

– et de diffuser plus largement une culture et une conscience du « risque cyber » au sein des administrations, par des actions de formation, de pédagogie et de prévention.

Le même constat et les mêmes conclusions s'imposent s'agissant des collectivités territoriales. Cela vaut notamment pour les collectivités les moins importantes. Un premier travail pourrait être mené avec leurs associations représentatives : Régions de France, Assemblée des départements de France, Association des maires de France, Association des petites villes de France.

Les acteurs économiques, en particulier les PME et les ETI, doivent également être mieux accompagnés. Cela passe d'abord par une évolution des mentalités. La protection contre le risque cyber ne doit pas être vue uniquement comme une contrainte et une charge financière. En réalité, elle contribue à la performance économique globale. Elle doit être considérée comme un investissement et une assurance, qui permettent notamment de prévenir le « risque de réputation » en cas d'attaque réussie. Le degré de cyber–protection constitue en définitive un avantage compétitif pour une entreprise, sur son marché national comme à l'export. Une telle prise de conscience est d'autant plus importante que l'usine 4.0 intégrera massivement les technologies numériques dans ses processus de fabrication et sera, par nature, à risque.

Afin de répondre à un certain nombre de ces enjeux, notamment s'agissant des petites collectivités et des PME, nous pensons que le réseau régional de l'ANSSI devrait être renforcé. Actuellement, un délégué de l'ANSSI doit être présent dans chacune des 13 régions métropolitaines. Cela semble insuffisant au regard des enjeux. Par ailleurs, ce réseau n'existe que dans l'hexagone, aucun délégué ne représentant l'ANSSI dans les outre-mer. Il est nécessaire, à terme, d'y remédier.

Enfin, les citoyens eux-mêmes doivent évidemment prendre davantage conscience du risque cyber. Chacun, à son niveau, doit être acteur de sa propre cybersécurité et participer ainsi à la résilience globale. C'est pourquoi il importe d'éveiller tous les citoyens à la « cyber-hygiène ». Nous suggérons plusieurs pistes de réflexion dans ce domaine. Nous préconisons ainsi la création d'une nouvelle filière menant à l'obtention d'un CAPES d'enseignement numérique, dont les titulaires formeraient les élèves par le biais d'enseignements spécifiques. Cet enseignement à part entière comprendrait, outre celui de la matière informatique, un éveil à la « cyber-hygiène » ainsi que l'enseignement des langages informatiques et de la programmation.

Au-delà de son bien-fondé intrinsèque, cet enseignement aurait l'avantage de développer des compétences transverses dont, par exemple, la capacité d'analyse, la logique et la résolution de problèmes. Il permettrait également de démystifier la matière et d'attirer plus de filles vers les métiers du numérique, qui demeurent aujourd'hui majoritairement masculins.

Des initiatives sont également envisageables à destination du citoyen consommateur et utilisateur de technologie. Alors que les enfants disposent de leur premier téléphone mobile à l'âge de 11 ans en moyenne, nous pensons que l'emballage et la notice d'utilisation de chaque produit technologique et numérique grand public devraient être complétés par une liste des principaux risques et mises en garde associés à leur usage.

Notre troisième série de recommandations vise à consolider une base industrielle et technologique de défense cyber. Car le cyber irrigue évidemment le champ de la conception, de la production et de la maintenance des systèmes d'armes et équipements qui ont vocation à être opérés par les armées. Cet aspect doit être pris en compte nativement dans les programmes d'armement, à plus forte raison dans le contexte de la numérisation croissante de l'environnement de combat. En effet, comme l'ont rappelé nos collègues Becht et Gassilloud, la numérisation des armées accroît mécaniquement leur surface d'exposition au risque cyber.

Nous estimons tout d'abord essentiel d'inciter à la « cyber–solidarité » au sein de la BITD. Celle-ci doit se matérialiser par un soutien plus prononcé des grands groupes à leurs chaînes de sous-traitants. Il peut prendre la forme d'actions de sensibilisation, mais également d'un soutien technique et financier pour assurer la « montée en gamme » de l'ensemble de la chaîne de la BITD. Des négociations et des accords pourraient être conclus avec les groupements industriels. L'État aurait un rôle moteur, voire contraignant, à jouer dans les groupes et entreprises au sein desquels il détient des participations, parfois majoritaires.

Une manière, plus contraignante, de développer cette solidarité consisterait à établir la responsabilité du donneur d'ordres sur l'ensemble de sa chaîne de sous-traitants en matière cyber.

M. Bastien Lachaud, rapporteur. S'agissant du financement de cette « montée en gamme » des sous-traitants, nous suggérons la constitution d'un « fonds cyber ». Il pourrait être alimenté par des contributions des acteurs de la BITD, mais également par une partie des recettes tirées des exportations d'armement réalisées par l'industrie française. Un taux de retour pourrait ainsi être déterminé chaque année en fonction des recettes réalisées l'année précédente.

Il convient également d'établir et de mettre à jour régulièrement une cartographie fine des entreprises et compétences critiques au sein de la BITD. Cela permettrait, d'une part, de les sécuriser de manière satisfaisante au niveau « technique » et, d'autre part, de les sécuriser « économiquement », en empêchant si nécessaire les prises de participation par des capitaux étrangers. Il convient donc de faire un usage, raisonné mais assumé, des dispositions prévues par le décret de 2014 relatif aux investissements étrangers soumis à autorisation préalable. Au–delà de la seule BITD, il pourrait même être envisagé de renforcer ce dispositif s'agissant de certaines entreprises du secteur de la sécurité des systèmes d'information.

Naturellement, il est nécessaire de continuer à soutenir et investir dans l'élaboration de solutions tant défensives qu'offensives. Pour les premières, il faut notamment maintenir l'effort dans les domaines de la cryptographie et du chiffrement. C'est essentiel au regard des ruptures technologiques à venir. Nous pensons en particulier au calcul quantique et au développement de l'intelligence artificielle qui accéléreront et faciliteront les opérations de déchiffrement.

Quant aux secondes, elles sont indispensables à plus d'un titre. Le cyberespace étant un espace de confrontation, nos armées doivent être capables d'y mener des actions, comme dans les milieux traditionnels. Par ailleurs, la détention de capacités offensives produit un effet dissuasif à l'encontre de ceux qui chercheraient à agir contre la France, ses citoyens et ses intérêts. Enfin, les connaissances acquises à l'occasion du développement de solutions offensives permettent, parallèlement, d'améliorer les postures défensives.

Sans que cela soit contradictoire avec ce qui précède, nous proposons d'améliorer la régulation de certains produits pour limiter la prolifération des technologies offensives et contrer les risques cyber systémiques. Cela suppose d'abord de mieux connaître les potentielles « armes numériques ». Une analyse fine et régulièrement mise à jour devrait permettre de déterminer les produits et technologies qu'il faudrait soumettre aux régimes encadrant les exportations ou transferts d'armements et de biens à double usage.

Un autre levier de régulation consisterait à envisager, sur le modèle applicable à certains matériels de guerre, la prohibition de l'emploi, de la fabrication et du commerce de certains produits et logiciels. Seraient concernés ceux qui seraient considérés comme les plus « dangereux », notamment ceux qui pourraient engendrer des risques et des dommages systémiques. Nous sommes conscients de la difficulté technique et juridique d'une telle initiative. Néanmoins, une analyse de la faisabilité d'une telle interdiction, qui viserait les « armes informatiques à effets massifs » pourrait utilement être entreprise, en concertation avec nos partenaires européens et internationaux.

Notre quatrième champ de préconisations vise à ajuster la « ressource humaine cyber », compte tenu des besoins actuels et prévisibles. Le cyber est un domaine dual en pleine expansion, qui intéresse à la fois le secteur civil et le monde militaire. Le « marché de l'emploi cyber » est aujourd'hui extrêmement tendu, ce qui nécessite la mise en œuvre d'actions résolues afin de renforcer, d'attirer et de fidéliser la « ressource humaine cyber », notamment au sein des autorités publiques qui en dépendent.

La première mesure consiste à faire connaître les différents métiers et formations du cyber. D'après les informations qui nous ont été communiquées, le taux de remplissage des filières faisant l'objet d'un suivi n'est que de 76 %, alors que les débouchés professionnels sont pour ainsi dire garantis. Des actions de communication ambitieuses pourraient donc être entreprises au niveau des établissements de l'enseignement secondaire, dès le lycée, et supérieur.

Une autre mesure est l'augmentation du nombre de places offertes dans les formations « cyber ». Les dernières études publiées estiment ainsi que notre pays accuse un déficit de 6 000 postes dans ce domaine.

Nous jugeons également nécessaire de renforcer les moyens humains et budgétaires de l'ANSSI, au-delà de la question de son réseau territorial précédemment évoqué. Il est vrai que l'ANSSI a déjà bénéficié d'efforts substantiels dans un contexte de réduction tendancielle de la dépense et du nombre d'agents publics. Toutefois, il est évident que les besoins vont se renforcer à l'avenir et qu'il convient donc d'anticiper cette évolution.

Il est intéressant de noter que l'agence allemande équivalent de l'ANSSI, le BSI, compte près de 55 % de personnels en plus, avec 850 agents environ. Or cette différence est sans rapport avec les écarts objectifs de population, la structure institutionnelle, la réalité socio-économique des deux pays, ou encore le niveau de menace cyber à laquelle nos deux pays sont confrontés. Dans l'idéal, l'ANSSI devrait disposer de moyens humains au moins équivalents à ceux du BSI. Cela permettrait de renforcer les capacités de réponse face à une crise majeure, d'accompagner efficacement l'ensemble des acteurs, de mener l'ensemble de ses missions sur un spectre qui aura été élargi par la LPM 2019-2025, et de constituer l'un des acteurs de premier plan aux niveaux européen et international.

Au-delà de la seule question quantitative, les autorités publiques doivent adapter leurs méthodes de gestion des ressources humaines afin de fidéliser les personnels du cyber. Toutes les personnes auditionnées l'ont souligné : si l'État n'éprouve pas de difficultés particulières à recruter et continue à attirer les talents, il lui est moins facile de les fidéliser, notamment au regard des niveaux de rémunération offerts par le secteur privé.

L'État ne sera probablement jamais en mesure de concurrencer les grandes entreprises dans ce domaine. Mais il peut s'efforcer d'offrir des perspectives de carrière plus nombreuses et plus variées. Cela passe notamment par le fait de favoriser les passerelles entre les différents services concernés. Un tel rapprochement serait bénéfique :

– aux personnels, en favorisant la mobilité et les perspectives de carrière ;

– et aux services eux-mêmes en facilitant les échanges, la diffusion d'une culture et de bonnes pratiques communes, la proximité opérationnelle, la mutualisation des outils et des équipements, etc.

À cet égard, nous pensons qu'une politique intégrée pourrait être mise en œuvre en matière de ressources humaines et de formation entre les différents acteurs de la chaîne cyber. Nous préconisons ainsi d'étudier la création d'une École de cyberdéfense. Elle rassemblerait les capacités de formation et d'entraînement pour l'ensemble des métiers cyber et pour l'ensemble des services et ministères concernés au premier chef, voire pour l'ensemble des administrations gouvernementales. Cette école permettrait le développement d'une culture partagée et favoriserait, par la suite, les passerelles entre les différentes institutions, contribuant ainsi à la fidélisation de personnels. Il faut souligner que le Royaume-Uni s'est récemment engagé dans une voie similaire avec sa *Defence Cyber School*.

Enfin, notre pays doit jouer un rôle moteur pour assurer les conditions de la cybersécurité collective au niveau international. La France doit développer son influence normative à l'international afin de promouvoir son modèle et ses valeurs, et ainsi proposer des alternatives à des positions qu'elle ne partagerait pas. On peut penser au concept américain de « légitime défense préventive », totalement étranger à la pensée française. On peut également évoquer le concept de *hack back*. Celui-ci consiste à reconnaître à un acteur privé victime d'une cyberattaque le droit de se faire justice lui-même, et de mener en représailles des actions cyber-offensives. Or une telle reconnaissance pourrait prospérer si l'on n'y prend garde, au risque déstabiliser encore davantage le cyberespace. Sans parler du fait qu'elle contreviendrait au monopole de l'exercice de la violence légitime par les États.

Naturellement, il est important que la France continue de travailler dans les instances internationales à l'émergence d'un corpus juridique partagé. En effet, le meilleur rempart contre les cyberattaques les plus massives reste la construction d'un environnement juridique accepté par tous les acteurs du jeu international et qui s'accorderaient sur le non-recours à certaines pratiques.

Enfin, il faut continuer de promouvoir la coopération internationale en matière cyber. À cet égard, il semble nécessaire d'envisager la cyberdéfense de la même manière qu'a été envisagé le contre-terrorisme, à savoir par le partage des données et de l'analyse des menaces. Cela passe par la conclusion ou l'approfondissement d'alliances pour partager, en temps réel ou quasi-réel, les caractéristiques des principales attaques. Dans le domaine cyber comme dans les autres, la coopération doit être conduite de manière lucide, sans naïveté. Mais face à un phénomène global, la coopération entre États n'est pas une option. C'est une nécessité.

Le cyber transcende les secteurs et les frontières nationales. Nous sommes la preuve qu'il transcende également les frontières politiques, puisqu'une rapporteure de la République en Marche et un rapporteur de la France Insoumise ont réussi à élaborer un rapport consensuel, tant au niveau des constats que des préconisations !

Telles sont les lignes directrices qui ressortent de nos travaux. Nous vous remercions.

M. le président. Je ne sais pas si c'est un miracle mais, en tout cas, c'est une réalité. Il y a vingt-deux questions, mes chers co-rapporteurs et chers collègues. Je vais commencer par les autres membres de la mission d'information.

M. Thibault Bazin. Je veux tout d'abord saluer le travail des deux co-rapporteurs et leur implication dans cette mission. Nous avons eu beaucoup d'éléments d'information.

D'abord, la menace cyber est réelle, en nombre et en intensité, avec des risques en termes de pertes de contrats, de marchés, de confiance, d'image, de protection et de performance. Les citoyens, les entreprises et les institutions ne sont pas assez « cyber-conscients ». Une hygiène numérique est nécessaire. Il n'y a pas assez de procédures de dépôt de plaintes. Il se pose également la question de la transparence pour mieux détecter les failles.

Nous avons eu des témoignages indiquant qu'on ne peut faire confiance à personne, même à nos amis et voisins. La réalité est qu'il est indispensable de protéger les systèmes d'inventions mais, surtout, cela a été dit, les données.

Les co-rapporteurs ont raison de questionner notre souveraineté. Des pans entiers d'infrastructures et d'applications informatiques sont dominés par des monopoles américains et chinois. De même, les technologies de « cyber-protection » sont largement dominées par les Américains.

Face à cela, la France ne dispose pas de produits souverains dans le domaine de l'antivirus, de l'« anti-malware » ou de « *sand boxes* », ces mécanismes permettant de détecter les « malwares ». Pour rattraper le retard pris, il est nécessaire de consacrer des moyens pour favoriser le développement de solutions françaises.

Il y a aussi un besoin de « *cloud* » étatique souverain et de serveurs en Europe. En effet, c'est le cadre juridique qui protégera la donnée estimée souveraine. Pour cela, l'opérateur de *cloud* doit se trouver sous juridiction française.

En matière de ressources humaines, la répartition des effectifs sur l'ensemble du territoire constitue un autre défi essentiel. Aujourd'hui un vrai pôle qualitatif existe en Bretagne, mais il est nécessaire d'avoir des pôles de formation sur tous les territoires.

Enfin, nous devons monter en puissance en matière de cyber-offensive et de cyber-riposte afin de pouvoir aveugler l'adversaire sur les théâtres d'opération contestés.

M. Philippe Michel-Kleisbauer. Merci de m'avoir accueilli en cours de route dans cette mission. Partie prenante de la commission « Science et technologie » de l'Assemblée parlementaire de l'OTAN, qui traite de ces questions, il était opportun que je suive avec vous ces travaux.

Dans le meilleur des cas, les cyberattaques sont simplement coûteuses. C'était le cas de « NotPetya » en Ukraine qui, en contaminant un logiciel de compatibilité, a touché un groupe français, Saint-Gobain, qui a provisionné 250 millions d'euros de pertes à l'automne,

et peut-être davantage. Cela avait été le cas de « Cabarnak » qui avait touché le système de virement « Swift » avec détournement de plus d'un milliard de dollars.

Les cyberattaques peuvent également consister en un grave sabotage tel que Stuxnet qui visait les centrifugeuses d'enrichissement d'uranium en Iran. Les cyberattaques peuvent aller très loin dans la déstabilisation. Ainsi en Ukraine, des comptes Facebook de soldats sont détournés pour créer une dissonance cognitive grave qui déstabilise l'armée. Enfin, vous y avez fait référence, la Revue stratégique de cyberdéfense envisage le fait que, très rapidement, ces cyberattaques puissent devenir létales.

Je souhaite savoir si vous avez abordé dans votre rapport la question du déni d'accès aux technologies permettant des cyberattaques à ceux qui ne disposent pas encore de ces technologies, qu'il s'agisse de personnes physiques ou de personnes morales, privées ou publiques, et notamment des États ?

M. Yannick Favennec Becot. Dans le rapport, vous préconisez un « cyber-enseignement ». Je souscris totalement à cette volonté. À partir de quelle classe, de quel âge peut-on préconiser ce « cyber-enseignement » ?

Mme Patricia Mirallès. La mission d'information a permis de dessiner une cartographie de la cyberdéfense au niveau de la France. À Montpellier, nous avons aussi un diplôme sur la cybercriminalité. Par ailleurs, la ville de Montpellier aide beaucoup les start-up innovantes en matière de problématiques de cyberdéfense.

Je souhaite poser trois questions. Comment améliorer l'accompagnement de l'innovation par l'ANSSI et la Commission nationale de l'informatique et des libertés (CNIL) afin de faciliter la certification des nouvelles technologies pouvant bénéficier à la défense qui sont développées dans le secteur privé ?

Quid d'un fonds d'investissement souverain pour l'innovation en matière de technologie, à l'image du fonds In-Q-tel financé par la NSA ou du fonds Libertad ?

De quelle manière l'agence pour l'innovation créée en mars 2018, qui s'oriente avant tout vers l'intelligence artificielle (IA), pourrait comprendre un département « cyberdéfense » ?

Mme Marianne Dubois. Hier s'est tenue la seconde édition du forum « Cyberdéfense & Stratégie » au Cercle national des armées sur le thème « Quelles ruptures et quelles innovations pour la cyberdéfense ? ». L'IA et l'hyperconnectivité ont été au centre des discussions. Que pensez-vous de la tenue de ce genre de colloques sur des sujets aussi pointus et confidentiels, comme les capacités d'action futures dans le cyberespace et les outils et les dispositifs d'innovation en matière de cyberdéfense ? Est-ce qu'on peut légitimement débattre de ces sujets dans un colloque en toute confidentialité et en toute sécurité ?

M. Olivier Becht. Dans le combat permanent du glaive et du bouclier, l'arme du cyber dispose à la fois de la faculté de percer le bouclier et de neutraliser le glaive.

Avez-vous abordé la question de la résilience, notamment au niveau des OIV ? Si oui, quelles conclusions en tirez-vous ?

En effet, aujourd'hui, si les « bombes logiques » sont mises dans les composants d'un certain nombre de systèmes numériques, un risque important de ne pas pouvoir s'en prémunir par les systèmes de pare-feu existe. Les chinois sont aujourd'hui en train de doubler complètement leur système électrique pour faire en sorte que tous les systèmes d'électricité puissent fonctionner en manuel et hors numérique.

M. Joaquim Pueyo. Je voudrais bien évidemment saluer le travail des deux rapporteurs. Toutefois vous avez abordé trop rapidement, à mon sens, la question de la coopération européenne. Je pense en effet que les pays de l'UE, et je parle sous le contrôle de la présidence de la commission des Affaires européennes, devraient davantage travailler ensemble en matière de cyberdéfense suite aux cyber-attaques multiples et croissantes contre des cibles civiles et militaires. Ne pensez-vous pas que les États membres devraient renforcer la capacité de collaboration de leurs forces armées et améliorer la cyber-coopération au niveau européen ? Que pensez-vous également d'une meilleure coopération avec l'OTAN ? Car je crois savoir qu'entre la France Insoumise et l'OTAN, on ne peut pas parler d'une grande amitié… Puisque vous avez parlé de « coopération », je serais d'avis d'aller jusqu'au bout en la matière. Enfin, ne pourrions-nous pas intégrer d'autres partenaires ? Certains pays ont en effet de bonnes connaissances sur le sujet, l'Allemagne et le Royaume-Uni, par exemple.

Dans le cadre de la coopération structurée permanente, quel est votre point de vue concernant le lancement du cyber-projet relatif à la mise en place d'une plateforme d'information sur les cyber-incidents ? Celle-ci mettrait également à disposition des équipes pouvant intervenir rapidement en cas de problèmes informatiques. Il s'agirait donc de partager nos compétences et nos connaissances dans le domaine du numérique sur une plateforme d'envergure européenne.

Ce sont des questions qui m'intéressent car vous avez certes soulevé des problèmes de fond, mais je pense que nous ne pourrons pas travailler correctement et efficacement intra-muros, c'est-à-dire cloisonnés dans un contexte purement hexagonal.

M. Jacques Marilossian. Je souhaiterais revenir sur la manière de faire émerger une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires mais aussi sur les réseaux de la réserve. Le Pacte de cyberdéfense de 2004 prévoyait de développer une réserve de cyberdéfense à vocation opérationnelle pour assister l'État et les armées en cas de risque majeur. Ce projet, développé en étroite coopération avec l'ANSSI et la gendarmerie nationale, prévoit que la réserve comprenne 4 440 personnes en 2019 soit 40 postes permanents, dont une vingtaine en régions et outre-mer. Elle comprendrait également 400 réservistes opérationnels dont 200 en régions et outre-mer et 4 000 réservistes citoyens, mobilisables sur l'ensemble du territoire national. Que pensez-vous de la situation de la réserve de cyberdéfense aujourd'hui et de son avenir ?

Mme Laurence Trastour-Isnart. Le cyberespace est devenu un domaine stratégique et au vu de l'intensification des attaques informatiques et des cyber-menaces, on peut aujourd'hui parler de « cyberguerre ». Vous avez évoqué les start-up qui ont une place stratégique et essentielle dans l'innovation, avez-vous pu analyser la part du budget consacrée à la R&D spécifique au domaine de la cyberdéfense ?

M. Christophe Blanchet. Vous proposez dans votre rapport l'idée d'une grande loi concernant la cyber-sécurité et je partage totalement votre avis quant à cette proposition.

J'avais d'ailleurs déjà évoqué cela auprès du ministère en décembre dernier et je suis convaincu qu'il y a une véritable urgence à agir. À présent, pensez-vous qu'il soit du ressort et du devoir de la représentation nationale de légiférer en ce sens ? Avons-nous le temps d'attendre un projet de loi ou devons-nous écrire une proposition de loi ensemble ? Enfin, quelle devrait être la position de notre commission vis-à-vis de ces initiatives ?

M. Christophe Lejeune. Il y a deux jours, le commandant de la base de défense de Nancy a signé un contrat pour l'installation d'un laboratoire d'entraînement en matière de cyberdéfense, qui sera implanté à la caserne Verneau pour des questions évidentes de sécurité. Ce laboratoire fait partie du dispositif de cyberdéfense voulu par le Premier ministre, doté, à l'échelon national, de 300 ingénieurs. Ce laboratoire, qui fera notamment appel à des réservistes opérationnels, s'appuiera sur un partenariat avec Cyber-Detect et Airbus.

En matière de cyberdéfense, il est fondamental de s'assurer du parcours sur le long terme des futurs opérateurs, ainsi que vous l'avez d'ailleurs évoqué dans votre rapport.

Aussi le recrutement est-il particulièrement pointu, utilisant des critères militaires de sélection. La deuxième phase de développement de cet outil indispensable serait ensuite la finance et la santé. Le Grand Est est d'ailleurs une aire d'importants flux financiers. Ma question est donc la suivante : le problème majeur demeurant le recrutement, la mise en place de dispositifs indemnitaires particuliers pour faire face aux salaires élevés du civil est-elle envisageable ?

Mme Émilie Guerel. La cyber-sécurité est un sujet hautement sensible dans la sphère aérienne. Aussi, j'aimerais savoir si, réellement, un avion a déjà fait l'objet d'une cyber-attaque. En 2013, un chercheur spécialiste du hacking a évoqué la possibilité de pénétrer les cockpits d'avions, mais n'a jamais pu en apporter la preuve. En 2015, un autre chercheur assurait être parvenu à hacker le système de divertissement d'un avion de ligne mais sans en apporter, là encore, la confirmation. Lors de la dernière conférence *Black Hat* (réseau de conférences sur la sécurité de l'information), un hacker a évoqué la possible pénétration du système d'information d'un avion de ligne en vol en utilisant ses communications satellites. J'aimerais donc savoir si ces menaces sont réelles et réalistes et, si oui, de quelle manière la France s'en prémunit-elle ?

M. Charles de la Verpillière. Ma question concerne ce que vous avez appelé les OIV, c'est-à-dire les « opérateurs d'importance vitale ». On pense évidemment à tout ce qui concerne l'électricité avec EDF, RTE pour le transport et la distribution, la SNCF, les syndicats des eaux, les opérateurs de communication et les hôpitaux. Avez-vous le sentiment qu'il y a désormais chez tous ces opérateurs une certaine prise de conscience quant aux questions de cyber-sécurité et, qu'en conséquence, des mesures efficaces ont été prises ?

M. Jean-Philippe Ardouin. La Revue stratégique de la cyberdéfense, publiée le 12 février 2018, met en lumière le danger des attaques informatiques susceptibles de porter gravement atteinte aux intérêts de notre pays. Il convient de développer et de structurer le dispositif national de protection notamment contre l'espionnage informatique et la cybercriminalité. La France inscrit son modèle de cyberdéfense dans une vision de stratégie européenne et internationale, notamment par le canal d'organisations telles que l'Union européenne, l'OTAN et l'ONU. Aussi, quels sont les accords internationaux s'appliquant dans

ce cas ? D'autre part, quelles sont les relations qui s'instaurent entre les différents protagonistes du numérique tels que les États, les acteurs publics et privés ?

M. Pieyre-Alexandre Anglade. Je tiens à saluer moi aussi la qualité du rapport qui nous est présenté. Je souhaite revenir, à la suite de notre collègue Joaquim Pueyo, sur la dimension européenne des enjeux de cyberdéfense. Comme les rapporteurs l'ont bien dit, le cyberespace ne connaît pas de frontières politiques ou juridiques ; c'est un espace aux contours impalpables, difficiles à cerner concrètement. En revanche, certains États y mettent en œuvre des stratégiques politiques et conduisent à cette fin, directement ou non, des actions visant à déstabiliser nos États et nos entreprises. Dans ce contexte de menaces asymétriques visant tous les États européens, l'Europe est en première ligne. En effet, s'il appartient à chaque État de mettre en place à son niveau des réponses à ces menaces, il nous faut aussi construire un véritable bloc européen, animé d'un esprit de souveraineté européenne dans le domaine cyber, face à d'autres grands blocs de puissances actives dans cet espace. La France a-t-elle l'ambition de jouer un rôle moteur en la matière ? Au fil de vos auditions, avez-vous perçu un mouvement collectif de prise de conscience européenne en ce sens ?

M. Alexis Corbière. On rappellera que l'Union européenne et l'OTAN coopèrent en matière de cyberdéfense alors que, comme vous nous l'avez bien dit, les États n'ont guère d'amis dans ce domaine. La France dispose avec l'ANSSI d'un outil de cyberdéfense relativement indépendant, mais poursuit-elle néanmoins des coopérations internationales en matière de cyberdéfense ? Avec quels autres États, et en quoi consistent-elles ? Par ailleurs, outre les coopérations déjà mises en œuvre, avec quels autres États la France aurait-elle intérêt à coopérer en ce domaine ?

Je tiens aussi à saluer le travail conjoint de nos deux rapporteurs ; merci pour ce cyber-moment.

M. Jean-Michel Jacques. On mesure bien quels progrès les Européens doivent encore accomplir pour atteindre un niveau technologique suffisant en matière cybernétique, notamment dans le traitement du *big data*. D'ailleurs, la DGSI sous-traite le traitement de certaines informations à une société américaine du nom de Palantir. Peut-être est-il difficile de développer un Palantir français ; mais, à tout le moins, ne faudrait-il pas soutenir le développement d'un Palantir européen ?

M. Fabien Gouttefarde. Ma question s'adresse particulièrement à notre collègue rapporteur Bastien Lachaud. En effet, si l'on passe en revue les compétences de pointe en matière de cyberdéfense, on ne peut pas ne pas évoquer le centre d'excellence de l'OTAN en matière de cyberdéfense, situé à Tallin. À vos yeux, vaut-il mieux pour la France trouver sa place au sein d'une telle organisation – même parrainée par l'OTAN –, ou se tenir en dehors, surtout quand on tient compte des enjeux de normalisation des standards technologiques pour la cybersécurité ?

Mme Séverine Gipson. Voilà un intéressant rapport, qui nous ouvre l'esprit. Fondamentalement, comment s'assurer qu'un système cybernétique est sûr ?

M. Thomas Gassilloud. Je salue la qualité du travail de nos rapporteurs ; même si notre collègue Alexandra Valetta-Ardisson y a peu fait allusion, nous nous connaissons depuis longtemps. J'en viens à ma question, qui s'inscrit à la suite de celles de nos collègues Pueyo, Anglade et Jacques. Le 6 juin dernier, la Commission européenne a annoncé le

lancement d'un plan d'investissement numérique de neuf milliards d'euros en faveur de l'Europe numérique. Outre les fonds destinés au développement du calcul intensif et de l'intelligence artificielle, ce plan prévoit un investissement de deux milliards d'euros dans la cybersécurité. Est-ce suffisant, et quels projets européens vous paraissent prioritaires, en complément de ceux des États membres ?

M. Laurent Furst. Vous avez évoqué les moyens limités de l'ANSSI : cette agence est aujourd'hui un service du Premier ministre ; ce statut juridique est-il satisfaisant ? Gagnerait-elle à un statut plus autonome ?

Par ailleurs, si l'on considère que le cyberespace constitue un milieu d'opération à part entière au sens militaire du terme, cela n'a-t-il pas d'implications juridiques, peut-être constitutionnelles ?

Enfin, on sait que pour nuire à un pays et le déstabiliser profondément, le plus efficace est de viser ses infrastructures énergétiques, mais aussi bancaires. Avec la numérisation croissante des opérations bancaires, cette vulnérabilité va en augmentant. Suffit-il à vos yeux de laisser aux banques le soin de se protéger seules, ou l'État doit-il agir ?

M. Philippe Chalumeau. À la lumière de vos travaux, dont je tiens à souligner la qualité, quelle appréciation portez-vous sur les dispositions de la loi de programmation militaire que nous venons d'adopter concernant la cyberdéfense ?

Par ailleurs, si cyberdéfense et cybersécurité sont bien deux domaines distincts, une étroite coordination entre ces deux champs d'action de l'État n'est-elle pas nécessaire ?

M. Florian Bachelier. Je m'associe aux félicitations adressées à nos deux rapporteurs, sans oublier notre collègue Thomas Gassilloud. Votre intervention met bien en exergue les nouvelles menaces et leur caractère hybride. Elle montre bien que la cybersécurité ne concerne pas seulement les armées, mais toutes les institutions, toutes les organisations. C'est en outre à juste titre que votre rapport replace ces questions dans l'optique de la souveraineté, y compris à l'échelle européenne.

Dans ce contexte, les Parlements eux-mêmes sont visés par des attaques de plus en plus nombreuses et de plus en plus dures. À cet égard, je tiens à signaler à nos collègues que l'Assemblée nationale a changé de doctrine et conclu un partenariat avec l'ANSSI pour mettre en œuvre des mesures de protection, dont la pose de sondes.

Ma question porte sur les nouvelles opportunités qu'offre le domaine de la cybersécurité : on évalue à trois millions le nombre d'emplois qui seront créés d'ici 2021 dans ce secteur en Europe. Comment mobiliser l'ensemble des filières de formation, notamment les filières courtes ?

Mme Alexandra Valetta-Ardisson, rapporteure. Mon collègue Bastien Lachaud et moi nous partagerons les réponses à ces questions, et même si certaines sont délicates, il y a une grande convergence de nos vues depuis le début de nos travaux.

Monsieur Chalumeau, s'agissant des moyens consacrés à la cyberdéfense dans la programmation militaire 2019–2025, il faut reconnaître que l'investissement consenti est très important et en adéquation avec les besoins et les demandes des acteurs concernés. L'ANSSI,

pour sa part, méritera une attention particulière. S'agissant de la coordination des efforts accomplis dans les champs civil et militaire, celle-ci est déjà à l'œuvre et mérite d'être approfondie.

Monsieur Michel-Kleisbauer, interdire l'accès de certains acteurs aux technologies permettant de mener des cyberattaques est par nature difficile, car il s'agit de technologies duales, avec lesquelles n'importe qui peut se muer en cyber-attaquant. Notre rapport présente des développements plus précis, mais pour faire simple, il faut certainement affermir autant que possible le cadre légal applicable et les contrôles. C'est pour cela que nous plaidons pour l'adoption d'une loi sur le cyber.

Quant au forum sur la cybersécurité dont j'ai prononcé le discours de clôture hier, il m'a donné l'occasion d'intéressantes discussions avec tous types d'acteurs. De tels événements ont l'avantage de favoriser une large prise de conscience des enjeux de cybersécurité, qui concernent la société dans son ensemble. Je ne doute absolument pas du respect du secret de la défense nationale par les autorités présentes. Enfin, ce type de rassemblement permet aux civils et aux militaires de se parler, ce qui est bénéfique.

Concernant l'Europe, notre collègue Bastien Lachaud va vous répondre en détail. Je tiens simplement à dire que je ne suis pas opposée par principe à des initiatives européennes, et j'estime que l'échelle européenne est bien sûr pertinente. Mais on sait comment l'Union européenne fonctionne : le consensus est la règle en de telles matières, mais il est souvent lent à mûrir, et rien ne garantit même qu'il soit possible. Le risque est donc qu'un texte européen sur la cybersécurité ne devienne l'arlésienne. Mieux vaudrait pour la France coopérer avec un nombre plus restreint d'États plus allants que les autres en la matière.

Monsieur Blanchet, l'idée d'une loi sur le cyber, qui formalise une doctrine française sur le cyber, nous paraît excellente. Cela répond d'ailleurs à une demande unanimement exprimée par les responsables que nous avons entendus. C'est pourquoi cette idée constitue la première de nos recommandations. Notre commission mériterait d'ailleurs à mes yeux d'être saisie au fond d'un tel texte, mais ce n'est pas à moi d'en décider !

Quant à l'idée de créer un enseignement sur le cyber dans la scolarité, qui tient particulièrement à cœur à Bastien Lachaud, elle vise à la fois à généraliser des pratiques de cyber-hygiène et à susciter des vocations pour les métiers du cyber.

Recruter des spécialistes du cyber est une nécessité, et les conserver, les fidéliser, en est une autre. Or les rémunérations offertes pour ce type de compétences dans le secteur public sont souvent insuffisantes pour cela. L'ANSSI ou nos armées investissent dans la formation de jeunes spécialistes du cyber, mais les industriels leur offrent au bout de quelques années des postes deux à trois fois plus rémunérateurs. Faut-il le regretter ? Peut-être pas, lorsque ces spécialistes sont recrutés par des industriels français ; mais c'est assurément plus regrettable lorsqu'ils quittent le service public pour de grands industriels américains du numérique. Le problème est aujourd'hui réel, et les autorités publiques en sont réduites à d'invraisemblables acrobaties administratives pour conserver leurs spécialistes du cyber. Notre rapport formule plusieurs propositions d'ajustements statutaires visant à mieux rémunérer les agents de l'État, par exemple au moyen de primes ou de contrats de droit privé.

Concernant les opérateurs d'importance vitale, ce sont les opérateurs les plus protégés du pays, dont les dispositifs de sécurité font l'objet d'audits réguliers. Mais le risque

zéro n'existe pas. Plusieurs de nos préconisations visent à réduire encore les risques, par exemple dans le cadre d'une loi sur le cyber, du développement de *clouds* souverains, ou de coopérations plus étroites entre le secteur public et le privé.

Madame Guerel, vous nous interrogiez sur la cybersécurité des avions. Nous avons entendu des représentants de l'industrie aéronautique et il en ressort que, ce secteur, comme d'autres, subit de multiples attaques. Mais ne soyons pas alarmistes : il y a différents degrés d'attaques et différents types de cibles. Des avions ont pu subir, par exemple, des attaques portant sur les systèmes de gestion des vidéos. Quant aux attaques portant sur les systèmes vitaux, les opérateurs concernés sont capables de les traiter.

M. Bastien Lachaud, rapporteur. Le Royaume-Uni a mis en place en 2014 un enseignement d'informatique dès l'école primaire, le Japon a prévu de faire de même au début des années 2020 pour tous les niveaux d'enseignement primaire et secondaire, et Israël a rendu un tel enseignement obligatoire au lycée. Selon nous, c'est le plus tôt possible dans la scolarité qu'il faut inculquer aux enfants les bonnes pratiques en matière cyber. Il suffit pour s'en convaincre de se rappeler que c'est en moyenne à onze ans que les jeunes Français se voient offrir leur premier téléphone intelligent : c'est avant cet âge qu'ils doivent être conscients des risques afférents à la protection de la vie privée et des données, ce qui contribuerait d'ailleurs à la lutte contre le cyber-harcèlement dans le secondaire.

S'agissant de la résilience de nos armées, Monsieur Becht, nos armements ne sont par nature pas invulnérables à des attaques cyber. Il est donc impératif que les nouveaux équipements soient systématiquement conçus pour pouvoir fonctionner en mode dégradé.

Concernant la coopération entre membres de l'Union européenne ou de l'OTAN, les États ont des capacités et des niveaux de compétence aujourd'hui très hétérogènes. Le risque est donc que des standards communs de protection soient moins ambitieux que les nôtres. De plus, un « bouclier cyber européen » pourrait même être contre-productif pour les États les plus vulnérables. En effet, il n'encouragerait pas ces États à développer leurs propres capacités de défense, alors même qu'un tel bouclier aurait nécessairement ses limites : en la matière, un peu comme pour la dissuasion, aucun État n'ouvre jamais la totalité de ses connaissances à ses partenaires, même les plus proches. Et ce n'est pas moi qui le dis, mais le directeur général de l'ANSSI. En somme, la coopération est nécessaire pour faire cesser les cyberattaques, mais on ne peut pas tout en attendre ; nous partageons des intérêts avec nos partenaires, mais la souveraineté reste la règle. Il existe à l'ONU une instance qui constitue un cadre approprié pour une telle coopération, le *Group of Governmental Experts*, mais celui-ci a dû interrompre ses travaux du fait de la défection des Russes et des Chinois. C'est dans un tel cadre que la France pourrait utilement faire la promotion de sa vision des rapports de droit international dans le cyberespace.

Quant à savoir s'il vaut mieux se placer au sein de l'OTAN ou en dehors pour faire prévaloir les vues françaises en matière de cybersécurité, encore faudrait-il que la France établisse une doctrine claire et que celle-ci trouve un écho parmi ses partenaires. Rien n'est certain en la matière. D'ailleurs, pour assurer le rayonnement d'une telle doctrine, les moyens dont dispose aujourd'hui notre ambassadeur pour le numérique, qui se limitent à trois collaborateurs, sont à l'évidence insuffisants.

En réponse à l'interrogation de Mme Mirallès sur la fiabilité des systèmes, les certifications délivrées par l'ANSSI permettent de s'assurer de la robustesse d'un produit. Nous formulons d'ailleurs le vœu, dans notre rapport, de conforter le processus de certification et de l'amplifier.

Pour revenir au plan de deux milliards d'euros proposé par l'Union européenne, la seule question qui vaille est : pour quoi faire ? Une nouvelle fois, nous avons le sentiment que l'argent est prêt à être dépensé mais qu'aucune stratégie n'a été établie afin de définir des priorités. Aujourd'hui, nul ne sait ainsi s'il faut investir dans la constitution d'un *cloud* européen ou dans un autre système. En somme, il est difficile de savoir si la somme engagée est suffisante dans la mesure où nous ne savons pas précisément ce qu'il faudrait financer.

Comme d'autres puissances, la France dispose de la capacité de mener des actions cyber-offensives dans le respect du droit international.

S'agissant du financement des activités de recherche et de développement, la loi de programmation militaire prévoit un investissement de 1,6 milliard d'euros. De plus, les entreprises investissent en moyenne entre 5 % et 8 % de leur chiffre d'affaires dans la sécurité de leurs systèmes d'information. Au-delà, nous n'avons pas eu accès à des informations plus précises, couvertes du reste par les dispositions législatives et réglementaires relatives au secret industriel.

La question de M. Pueyo me permet de rappeler que l'Union européenne dispose d'une agence spécialisée : l'ENISA (*European Network and Information Security Agency*). Cette agence a vocation à évoluer dans le cadre de la mise en place du système de certification à l'échelle européenne que j'évoquais précédemment. Pour la France, l'enjeu sera de veiller à ce que notre propre niveau de certification ne soit pas abaissé en raison d'un éventuel nivellement par le bas des normes de certification.

M. Marilossian nous a interrogés sur les réserves. Nous préconisons en effet un rapprochement des différentes réserves et le renforcement de leur rôle dans le cadre de la cyberdéfense.

Enfin, en réponse à l'interrogation de Mme Guerel, les flottes aériennes subissent quotidiennement des tentatives de piratage. Il semble relativement facile de *hacker* la bibliothèque de films mise à disposition des passagers. En revanche, accéder au système de navigation est beaucoup plus complexe, notamment parce que l'immense majorité de la flotte ayant été construite au début des années 2000, les avions sont assez peu connectés. Demain, les enjeux seront tout autres !

Pour conclure, j'évoquerai Palantir. Nous recommandons que les questions les plus sensibles restent protégées par les dispositifs garantissant la préservation de la souveraineté nationale. S'agissant de Palantir en particulier, il nous a été indiqué que lorsque les services de renseignement utilisaient les solutions proposées par cette société, une barrière hermétique était abaissée afin de garantir que les données ne s'échappent pas des serveurs sur lesquels le logiciel est installé. En d'autres termes, normalement la NSA n'a pas accès aux données de la DGSI. J'ajoute que les solutions de Palantir sont utilisées par divers acteurs, dont des avionneurs pour le traitement des données prédictives. Le mot de la fin sera la reprise du mantra de l'ensemble des acteurs rencontrés : en ce domaine, nous avons des alliés mais pas vraiment d'amis…

M. le président. Je remercie les rapporteurs pour toutes ces précisions et pour ce travail que l'ensemble de la commission semble avoir apprécié.

Mes chers collègues, dès lors que tout le monde s'est félicité de la qualité de ce rapport, je vous propose de le rendre public !

La commission autorise à l'unanimité le dépôt du rapport d'information sur la cyberdéfense en vue de sa publication.

La séance est levée à douze heures vingt.

*

* *

Membres présents ou excusés

Présents. - M. Damien Abad, M. François André, M. Pieyre-Alexandre Anglade, M. Jean-Philippe Ardouin, M. Florian Bachelier, M. Didier Baichère, M. Xavier Batut, M. Thibault Bazin, M. Olivier Becht, M. Christophe Blanchet, M. Jean-Jacques Bridey, M. Philippe Chalumeau, M. André Chassaigne, M. Alexis Corbière, M. Jean-Pierre Cubertafon, Mme Marianne Dubois, Mme Françoise Dumas, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Laurent Furst, M. Claude de Ganay, M. Thomas Gassilloud, Mme Séverine Gipson, M. Guillaume Gouffier-Cha, M. Fabien Gouttefarde, Mme Émilie Guerel, M. Jean-Michel Jacques, M. Loïc Kervran, Mme Anissa Khedher, M. Bastien Lachaud, M. Fabien Lainé, M. Jean-Charles Larsonneur, M. Didier Le Gac, M. Christophe Lejeune, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, M. Joaquim Pueyo, Mme Sabine Thillaye, Mme Laurence Trastour-Isnart, Mme Alexandra Valetta Ardisson, M. Charles de la Verpillière

Excusés. - M. Sylvain Brial, Mme Carole Bureau-Bonnard, M. Luc Carvounas, M. M'jid El Guerrab, M. Olivier Faure, M. Philippe Folliot, M. Christian Jacob, Mme Manuéla Kéclard-Mondésir, M. Jean-Christophe Lagarde, M. Franck Marlin, M. Gwendal Rouillard, M. François de Rugy, M. Patrice Verchère