ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Vendredi
15 octobre 2021
Séance de 9 heures

Compte rendu n° 32

SESSION ORDINAIRE DE 2021-2022

Présidence de
M. Thomas Gassilloud,
Rapporteur de la mission d'information

ASSEMBLÉE NATIONALE

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

Vendredi 15 octobre 2021

La séance est ouverte à neuf heures

(Présidence de M. Thomas Gassilloud, rapporteur de la mission d'information)

M. Thomas Gassilloud, président et rapporteur. Créée en 2009 et lointaine héritière de la direction nationale du chiffre, l'agence nationale de sécurité des systèmes d'information (ANSSI) est chargée de la sécurité des systèmes d'information de l'État ainsi que de ses opérateurs d'importance vitale. Au cours de nos auditions, nous avons pu constater l'importance prise ces dix dernières années par le niveau de sécurité informatique et par internet. Pour l'ensemble des acteurs concernés, la supervision et les préconisations de l'ANSSI représentent une forme de garantie ultime face aux menaces cyber, ce qui donne une idée de l'ampleur de vos responsabilités, qui s'étendent par ailleurs à la sphère économique en général et, de façon indirecte, à nos concitoyens, puisque l'ANSSI développe une politique active d'information et de recommandations auprès d'un large public.

Nous attendons de cette audition qu'elle nous aide à cerner précisément le concept de résilience en matière cyber, mais également qu'elle nous donne un aperçu des menaces, des scénarios de crise sur lesquels travaille l'agence et du degré de souveraineté auquel la France et l'Europe peuvent aspirer en matière numérique.

M. Guillaume Poupard, directeur général de l'agence nationale de sécurité des systèmes d'information (ANSSI). La cybersécurité est au cœur de notre métier. Un certain nombre de menaces ont comme point commun de passer par la voie numérique et nous faisons face à des adversaires qui visent véritablement à porter atteinte à nos systèmes numériques, de différentes manières. Notre rôle est de protéger au maximum les systèmes critiques français, ce qui peut concerner de nombreux acteurs. En réalité, aujourd'hui, chacun est concerné à son propre niveau. Le concept de résilience est lié au champ de la sécurité numérique. Nous faisons preuve de résilience depuis un certain temps sans même nous en apercevoir.

Nous faisons face à trois types de menace. La première est la menace criminelle, qui porte atteinte aux systèmes d'information et aux données des victimes pour les faire chanter et obtenir des rançons. Cela touche directement l'activité des entreprises, des collectivités locales, des hôpitaux, etc. Se pose donc la question des moyens à mettre en œuvre pour continuer à fonctionner et revenir à une situation normale, à travers la continuité d'activité et la reprise d'activité, qui sont les bases mêmes de la résilience. Force est de reconnaître que ce type de menace a littéralement explosé : multiplication par quatre du nombre d'attaques entre 2019 et 2020 et augmentation d'environ 60 % pour l'année 2021. Il s'agit donc de prévenir les victimes potentielles de cette menace, mais surtout de trouver des solutions afin de les en protéger.

L'espionnage, dont la perception est encore largement insuffisante, représente la seconde menace, aujourd'hui massive. Elle peut prendre des formes très diverses. Le risque peut être individuel, jusque sur nos smartphones, les décideurs en particulier représentant des

cibles potentielles via leurs téléphones personnels et professionnels. Le niveau de complexité et de perfectionnement des outils à disposition pour de tels actes est absolument incroyable. Le risque économique est par ailleurs bien plus important qu'on ne l'imagine. Il peut également s'agir d'espionnage stratégique, ayant des impacts potentiellement très graves sur nos capacités de résilience.

La troisième menace concerne les actions destructives menées *via* les systèmes numériques. Il est faux de penser que le virtuel n'a pas d'impact sur le réel. À travers le numérique, on peut toucher la plupart des systèmes physiques, les faire dysfonctionner, voire obtenir des effets absolument catastrophiques. La protection de ces systèmes certes physiques, mais qui se sont numérisés, constitue notre première priorité, sur laquelle nous devons investir maintenant afin de prévenir des catastrophes dans dix ans. Nous nous situons donc tout à fait dans une logique de résilience basée avant tout sur la prévention, mais nous imposons également aux opérateurs d'importance vitale, ainsi qu'aux opérateurs de services essentiels, une capacité à comprendre et à anticiper ce qui pourrait se passer au moment du retour à la normale. Or cette reprise d'activité est rarement anticipée, s'étalant en général sur une longue période, ainsi qu'on a pu le constater par exemple au sein des hôpitaux ces dix-huit derniers mois. Il s'agit donc d'un axe de travail important, d'autant que les risques à venir seront encore plus graves.

M. Thomas Gassilloud, président et rapporteur. Les incidents des derniers jours nous ont montré que les attaques pouvaient émaner d'une volonté délibérée, telles les attaques par déni de service distribué ou *Distributed Denial of Service* (DDoS), ou d'erreurs humaines comme on l'a vu chez Facebook et chez OVH en matière de routage. Au fil des attaques, on découvre des situations que l'on n'avait pas forcément anticipées, des vulnérabilités d'outils métiers, y compris de secteurs critiques. En Amérique du Sud par exemple, la panne de WhatsApp a fait réaliser à quel point cette application était utilisée au quotidien, aussi bien pour réserver un taxi que pour échanger avec les commerçants, par exemple. Selon vous, évaluons-nous correctement les impacts potentiels d'une indisponibilité des réseaux télécom pendant une heure, une journée, voire une semaine complète ?

M. Guillaume Poupard. Je suis personnellement convaincu que l'on sous-estime énormément les conséquences de ces dysfonctionnements. Par une analyse un peu trop superficielle, on est en mesure d'évaluer les effets directs et on se persuade que la situation serait gérable, mais les effets indirects sont très difficiles à anticiper. J'illustrerai mon propos par deux exemples aujourd'hui prescrits. Il y a plusieurs années, nous avions effectué une expérience au sein d'un hôpital. À cette époque, la dépendance à internet était nettement moins marquée qu'aujourd'hui. La question posée était la suivante : sans accès internet, quel serait l'impact sur votre fonctionnement ? Les projections de l'établissement conduisaient à une absence de conséquences. Un exercice concret a ensuite été réalisé et l'hôpital s'est rendu compte, à sa grande surprise, qu'il se trouvait dans l'incapacité de fonctionner au bout de deux jours. En effet, l'ensemble de la chaîne de nettoyage et de décontamination des équipements chirurgicaux était devenu dépendant d'internet.

Le deuxième exemple est celui des drones autonomes déployés en Afghanistan il y a quelques années. Un jour, subitement, ils ne décollent plus, sans que l'on comprenne pourquoi. En réalité, cette panne était liée à l'absence d'internet depuis plusieurs jours. Les chaînes de maintenance, auxquelles sont soumis tous les appareils numériques en général, avaient été interrompues, ayant pour conséquence la mise en état de sûreté des équipements, ce qui se traduisait ici par un refus de décoller. Pour le ministère des armées et pour la

direction générale de l'armement (DGA), cette expérience fut révélatrice du manque d'anticipation aux dépendances.

Je suis tout à fait certain que dorénavant, toute coupure d'internet ou d'accès à la 5G équivaudra à une panne électrique. Bien sûr, chaque analyse doit être effectuée au cas par cas pour affiner la notion de continuité d'activité. Il s'agit en effet d'identifier les dépendances et d'être en mesure de faire fonctionner ces systèmes critiques même sans internet. Il est toutefois inquiétant de constater que, dans de nombreux domaines, on perd progressivement cette maîtrise et on ne redécouvre les problématiques qu'au fil des attaques effectives.

M. Thomas Gassilloud, président et rapporteur. Le fonctionnement d'internet est dépendant de l'alimentation en électricité, mais vous nous indiquez aussi qu'une dépendance inverse est en train de s'installer, c'est-à-dire l'électricité tributaire des réseaux de télécommunications. Afin d'être en mesure d'évaluer correctement cette dépendance, pourrait-on envisager une forme de *stress test* qui consisterait à demander aux opérateurs d'importance vitale (OIV), un jour par an, par exemple, de fonctionner sans internet et d'en observer les conséquences ?

M. Guillaume Poupard. Je trouve cette idée excellente. En revanche, elle nécessite un niveau de maturité que de nombreux OIV n'ont pas encore atteint. Nous pouvons établir un parallèle très simple. Lorsqu'on met en place des secours électriques – batteries, alternateurs, etc.–, ces systèmes doivent être testés une fois par mois pour s'assurer de leur fonctionnement le jour où on en a besoin. Le même raisonnement peut s'appliquer pour internet. Tester ses plans de continuité d'activité en s'autorisant à couper réellement l'accès à internet, ne serait-ce que dix minutes, afin de vérifier si les systèmes critiques continuent à fonctionner, constitue à mon avis le test ultime de maturité. Ce type de test se pratique pourtant assez rarement. Si l'on s'intéresse à la question de la 5G, il est beaucoup plus difficile de trouver des alternatives qu'en cas de simple coupure électrique. Il faut donc avoir prévu des réseaux redondés pour les systèmes critiques, ce qui est à la fois complexe et coûteux.

M. Thomas Gassilloud, président et rapporteur. J'ai l'impression que, d'un point de vue psychologique, tant que la catastrophe n'a pas eu lieu, nous éprouvons collectivement des difficultés à l'envisager. Cette mission d'information pourrait servir à demander la réalisation de ces *stress tests*. Au-delà d'une simple mesure de notre dépendance à la technologie, ces derniers seraient intéressants d'un point de vue managérial. Au sein de mon entreprise, par exemple, nous avions instauré une journée sans utilisation de messageries instantanées, afin de développer des usages plus raisonnés tels que se lever pour interagir directement avec la personne concernée. Ces tests permettraient aussi de mesurer les investissements qui doivent être réalisés pour pouvoir fonctionner en mode dégradé. Récemment, on a manqué de blouses jetables dans le secteur médical, alors que l'utilisation de blouses en tissu comme cela se faisait avant réglait d'office le problème.

Plus globalement, je suis interpellé par le fait que les réseaux critiques tels que l'alimentation en énergie vont devenir de plus en plus dépendants d'internet, quand Enedis et EDF nous promettaient une stricte compartimentation des deux domaines. La contrepartie ne consisterait-elle pas à penser un internet relativement autonome, a minima en mode dégradé, à l'échelle française ou européenne ? Peut-on raisonnablement envisager cette option ou sommes-nous soumis à des dépendances techniques qui nous priveraient de la possibilité d'un tel fonctionnement ?

M. Guillaume Poupard. Si tous les OIV suivaient l'exemple d'EDF, le travail en serait facilité. Il est tout à fait naturel d'utiliser internet comme moyen de communication de base. Mais si cette ressource n'est plus disponible, il est important que les systèmes critiques portés par ces OIV ne s'effondrent pas simultanément. Il faut donc réussir à trouver un équilibre entre une dépendance totale à internet et la non-utilisation de cet outil, de la 5G ou des *clouds*. En revanche, l'analyse constante des dépendances est nécessaire de façon à éviter la catastrophe en cas de coupure.

L'internet français n'est pas autonome. Nous faisons partie d'une plaque mondiale. Les interconnexions sont clairement identifiées mais, si l'on coupait les câbles au niveau des frontières nationales, à l'intérieur plus rien ne fonctionnerait. Ce genre de problème n'est toutefois pas inéluctable. La Chine a conçu un internet autonome, aboutissement d'un travail de plus de vingt ans. La Russie, quant à elle, ne dispose pas d'un internet autonome mais communique régulièrement sur sa capacité, en cas de problème, à verrouiller les frontières et continuer à bénéficier d'un internet fonctionnant localement. Faut-il transformer l'internet français en sorte qu'il puisse fonctionner en autonomie ? Je n'en suis personnellement pas persuadé, dans la mesure où une telle vision irait à l'encontre des principes mêmes d'internet. D'un côté, nous sommes soumis à une forme de dépendance, ou de souveraineté partagée. De l'autre, en termes de résistance aux pannes et de résilience, internet est plutôt bien conçu. Rappelons que sa création repose sur la volonté de disposer d'un réseau résistant aux frappes nucléaires. Le principe absolument génial du maillage, c'est-à-dire la poursuite de son fonctionnement même lorsque certains chemins ne sont plus disponibles, est assez exceptionnel en termes de résilience. Nous avons probablement besoin, pour toutes les activités critiques, d'un « plan B » dissocié de l'utilisation d'internet et donc basé sur des technologies de secours, ce qui est coûteux mais extrêmement simple. En revanche, la duplication de réseaux internet autonomes ne me paraît pas pertinente.

M. Thomas Gassilloud, président et rapporteur. EDF utilise les réseaux de télécommunications pour ses équipes de maintenance, dispose de fait de passerelles vers internet, et se trouve donc exposé à des risques vitaux, y compris sur ses systèmes alternatifs. Nous assisterons bientôt au développement des *smart grids* qui vont conduire à une convergence entre énergie et télécommunications. Progressivement, notre volonté d'optimisation de nos moyens de production va nous rendre moins résilients. Le « plan B » que vous évoquiez est par conséquent absolument nécessaire. On pourrait même parler d'un « plan C » reposant sur l'acquisition d'une certaine autonomie des réseaux de télécommunications.

D'un point de vue politique, cela n'a jamais été envisagé en France ni en Europe, mais il me semble que nous devrions nous poser la question. En travaillant sur certains sujets sensibles, je réalise que parfois, dans des situations de crise, ce que l'on pensait improbable quelques années plus tôt devient inéluctable, à l'image du rétablissement récent des frontières au sein de l'espace Schengen. La question de l'autonomie d'internet mérite donc d'être posée.

À l'échelle des cinq puissances du Conseil de sécurité des Nations unies, qui sont dotées de capacités de dissuasion nucléaire, la Chine travaille sur une isolation de son réseau internet, la Russie y travaille également, et nous pourrions nous rassurer en pensant que nous, les démocraties occidentales, notamment les Américains, les Anglais et les Français, n'avons pas besoin d'y travailler. Cependant, on constate que l'internet français est dépendant. Si je vous demande si le réseau américain est dépendant du réseau français, je pense que vous me répondrez par la négative. Et quand on connaît la stratégie d'alignement des Anglais vis-à-vis des Américains, on réalise que l'on est peut-être le dernier pays du Conseil de sécurité à ne

pas se poser la question, dans un contexte où la pression d'un simple bouton, y compris de la part d'un allié, pourrait nous rendre tout à fait serviles. Les relations internationales se tendent et nos alliés les plus proches nous montrent qu'en cas de crise, ou quand l'essentiel est en jeu, ils sont en mesure d'actionner l'ensemble des leviers dont ils disposent. Par conséquent, je pense que cette question de l'autonomie n'est pas complètement en contradiction avec nos autres stratégies. Sinon, quelle est la raison d'être de Galileo ?

Nous avons par ailleurs auditionné les câbliers sous-marins, qui nous ont fait part des tensions sur le marché, notamment avec les GAFA – Google, Apple, Facebook et Amazon – et les BATX – Baidu, Alibaba, Tencent et Xiaomi –. J'en conclus que, petit à petit, nous allons assister à une convergence croissante des capacités d'hébergement, dans la mesure où nous allons réduire les coûts de transport de la data, et au développement d'un mode dégradé qui le sera de plus en plus, puisque les hébergements seront de plus en plus centralisés. Compte tenu de l'ensemble de ces arguments, est-il saugrenu de réfléchir à une autonomie stratégique en matière d'internet ?

M. Guillaume Poupard. Commençons par énoncer un principe évident : ne pas refuser l'évolution technologique. La sécurité serait effectivement plus facile à assurer sans cette dernière. Il faut plutôt accompagner les progrès technologiques en y associant une sûreté de fonctionnement qui se place au niveau des enjeux. Cela est valable même pour les secteurs critiques des grands opérateurs.

Je ne suis pas forcément le meilleur expert pour aborder les questions d'autonomie. J'ai le sentiment que pour certaines fonctions critiques, on gagnerait, en France et en Europe, à développer certaines technologies comme les DNS, sorte d'annuaires qui effectuent la transcription entre les adresses IP et les noms de domaines. Dans les pannes récentes, les DNS sont souvent impliqués. La criticité de ce genre d'équipement apparaît donc clairement, et le fait de disposer « en local » de répliques de ces équipements me paraîtrait extrêmement simple à mettre en œuvre. Si vous demandez à un DNS l'adresse IP d'un site connu pour être malveillant, géré par des attaquants, celui-ci vous aidera néanmoins à vous connecter à un tel site. Or il existe des contre-mesures assez simples qui consistent à retirer ces sites malveillants de l'annuaire. Je travaille actuellement à la création d'un tel DNS pour l'administration. Mais réaliser ce travail à l'échelle nationale pourrait constituer un très beau projet, avec une teneur politique qui ferait vraiment sens. Il ne s'agirait pas d'un pied de nez à nos amis américains, mais simplement de prendre nos responsabilités. Il n'est écrit nulle part que tout devait être centralisé aux États-Unis.

Je ne suis pas sûr qu'il faille penser internet à l'échelle européenne. Le web reste finalement une affaire de « tuyaux » qui appartiennent aux GAFAM. Cette dépendance à ces derniers sur des sujets qui ne sont pas historiquement les leurs m'inquiète quelque peu et doit constituer un motif de surveillance accrue. Il faudrait en effet éviter une sorte de privatisation de l'internet. Mais je ne maîtrise pas suffisamment le sujet pour m'avancer davantage.

Aujourd'hui se joue un débat à propos du *cloud* souverain. Sommes-nous condamnés à être dépendant des *clouds* américains et demain chinois, ou bien décidons-nous de devenir souverains en la matière et de développer nos propres solutions ? Cette question est paradoxalement beaucoup plus facile à aborder que le sujet d'internet qui, en tant que système de communication, par définition, se doit d'être partagé. Nos *clouds*, y compris chez nos OIV, consomment massivement des offres standard américaines qui sont probablement très fiables sur le plan de la sécurité technique mais qui, en termes de sécurité juridique, sont catastrophiques. Ces offres, sont soumises à la réglementation américaine, donnant accès à

toute l'administration – juges, services de renseignement, etc.– aux données contenues dans les *clouds*. Le droit américain utilise sa domination technologique pour en tirer des bénéfices, et ce de façon remarquable. L'enjeu est de savoir comment faire pour nous assurer que nos systèmes et données critiques ne sont pas en risque vis-à-vis de ce droit américain et vis-à-vis du droit chinois demain. Deux pistes s'ouvrent alors : la première est de disposer de nos propres solutions, ce qui est beaucoup plus facile dans ce domaine que dans celui d'internet, les acteurs européens en la matière étant par ailleurs juridiquement sûrs. La seconde serait de continuer de bénéficier de la technologie américaine, qui en soi n'est pas dangereuse. Cela peut s'effectuer à travers la mise en place de projets, l'un avec Microsoft, Capgemini et Orange, qui consiste à faire opérer la technologie Microsoft par un acteur qui n'est pas soumis au droit américain, l'autre avec Thalès et Google, basé sur un principe identique.

Cette piste a peut-être un sens au niveau national, mais j'en doute. Elle prend en revanche tout son sens au niveau européen. Aujourd'hui, je suis inquiet de constater qu'à l'échelle européenne, il existe une différence de culture et de sensibilité sur ces problématiques. Il s'agit d'un sujet politique au sens le plus fondamental du terme : l'Europe est-elle capable d'assumer le fait que ses systèmes et données critiques doivent être uniquement soumis au droit européen ?

M. Thomas Gassilloud, président et rapporteur. La prise de conscience de ce sujet est en elle-même une avancée. Il faut rassurer tout le monde sur le fait que l'on ne mélange pas les objectifs. Si les Chinois veulent assurer leur autonomie, c'est certainement avant tout pour maîtriser les flux informationnels. Au contraire, les démocraties peuvent travailler sur le sujet de l'autonomie pour la résilience en garantissant qu'il n'existe, bien entendu, aucune volonté de maîtriser le contenu en tant que tel et de porter atteinte à la neutralité du net. Par ailleurs, l'objectif final n'est pas de se vanter de posséder un internet autonome, mais bien d'avancer en termes de DNS, de pouvoir détecter les flux sans intervenir dessus et éventuellement de disposer d'une capacité de blocage ciblé. Il s'agit simplement d'adapter nos dispositifs au niveau de la menace. Se l'interdire serait irresponsable.

L'ANSSI a grandement contribué à faire avancer la réflexion sur le *cloud* de confiance. On voit bien que les démarches nationales, qui étaient binaires, qui voulaient absolument impulser un acteur français, ont été rattrapées par la réalité. Modération et humilité sont donc deux valeurs indispensables dans ce domaine pour viser l'efficacité. Néanmoins, il est assez inquiétant de constater qu'Airbus, la direction générale de la sécurité intérieure (DGSI) ou encore Thalès, d'une certaine manière, se résignent à une telle approche. Cette résignation ne me semble acceptable et soutenable que si l'on ne franchit pas le point de non-retour. Certes, on va se prémunir du droit américain, mais par ailleurs on va contribuer à accroître l'adoption de technologies qui ne seront jamais souveraines. Je me désole de l'absence de fixation de clauses de retour technologique. Lorsqu'on vend des sous-marins ou des Rafale, il est toujours question de transfert de technologies. N'existe-t-il pas un risque d'irréversibilité dans une telle approche ?

M. Guillaume Poupard. Le point de vue pessimiste nous conduirait à considérer que la question ne se pose plus en ces termes : nos OIV utilisent tous des *clouds* américains selon des offres standard, absolument pas souveraines et absolument pas maîtrisées sur le plan juridique. La situation existante est donc déjà mauvaise. Nous devons en tenir compte.

Mon seul regret, finalement, c'est qu'en termes de marketing ou de lobbying, l'image des offres américaines et chinoises est meilleure que celle des acteurs européens ou nationaux, qui présentent pourtant de vraies qualités. Il faudrait leur donner leur chance. D'ailleurs, ceux

qui le font sont agréablement surpris, car ils répondent à la majorité des besoins, et ce de façon excellente. Reste le cas des opérateurs qui souhaiteraient profiter des technologies non européennes qu'ils ont pris l'habitude d'utiliser. C'est la raison pour laquelle cette démarche d'immunisation au droit américain me semble absolument indispensable. Elle reflète d'ailleurs les besoins exprimés par les directeurs des systèmes d'information (DSI) des grands groupes. Cependant, nous y parvenons difficilement, surtout lorsque les technologies impliquées sont complexes. Il existe en outre des offres qui, pour des raisons technologiques ou de contrats, sont complètement verrouillées. Le pire des exemples est celui des bases de données dans lesquelles, pour récupérer vos propres données, vous devez payer à la donnée. Ce sont des contrats qui n'ont pas été bien préparés au départ ou qui n'ont pas été compris, et les consommateurs, qui sont propriétaires de leurs données et ne sont toutefois plus en mesure de les récupérer, ce qui est totalement absurde.

Je reste convaincu que refuser la technologie européenne serait une erreur, de même que le fait d'assimiler la notion de souveraineté à l'origine de la technologie. Nos acteurs français utilisent et proposent de belles offres reposant sur de la technologie américaine, à l'image de l'association entre OVHCloud et Anthos – Anthos étant gérée par Google. À vouloir nous refermer sur nous-mêmes, nous risquons d'aboutir à des résultats très décevants, car nous aurons réalisé de beaux systèmes souverains qui finalement ne seront pas réellement utilisés.

Il s'agit toutefois un sujet très complexe, où l'on souhaite porter à la fois deux approches probablement contradictoires par certains aspects. D'un côté une offre purement européenne que l'on souhaite développer pour des raisons de souveraineté, de sécurité, mais aussi pour des raisons économiques. Et d'un autre côté, une offre hybride qui a le mérite de se situer dans la continuité de ce qui existe déjà ailleurs, qui est déjà appliquée, qui est meilleure en termes de sécurité mais qui ne confère pas de souveraineté absolue, et qui présente le danger de tuer la première offre. Ainsi que je le disais très récemment aux assises de la sécurité, nous nous situons sur cette ligne de crête où des positions trop arrêtées, bien que confortables, sont malheureusement inefficaces.

M. Thomas Gassilloud, président et rapporteur. J'ai le sentiment que la donnée est peu valorisée dans les entreprises et que, parfois, le fait de se tourner vers un concurrent étranger peut se faire uniquement en raison de son attractivité. D'après la doctrine des industries naissantes, formalisée dans l'économie, celles-ci sont des industries – je cite Wikipédia – « qui ne sont pas capables à l'origine de faire face à leur concurrence étrangère, du fait de leur manque d'expérience et de savoir-faire, mais qui le seraient à long terme, une fois ce savoir-faire acquis ». Politiquement, je serais presque prêt à assumer l'affirmation selon laquelle, au sein de la DGSI, il faudrait dégrader quelque peu le degré de sécurité des prochaines années afin de concentrer nos efforts dans le développement de notre propre système, qui nous protégera durablement, sur un horizon à plus long terme. Le juge de paix restant tout de même les montants investis dans la recherche et le développement.

Par ailleurs, le réseau radio du futur (RRF) a pour objectif de créer dans les prochaines années un système de communication sécurisé, résilient et pleinement interopérable. Les réseaux radio de la gendarmerie ont montré leur résilience par rapport aux réseaux télécom. Mais les doutes restent un peu les mêmes. Quelle est votre appréciation personnelle du RRF de nos forces de sécurité ?

Pour terminer, pourriez-vous nous parler du *cloud* de confiance ?

M. Guillaume Poupard. De nombreux acteurs n'ont pas encore compris que les données dont ils disposaient ainsi que leur capacité à les traiter constituaient le cœur de leur métier. Certains doivent évoluer très vite, comme les services de renseignement intérieur, et ils réalisent des efforts colossaux pour y parvenir. À titre d'exemple, quand on fabrique des avions aujourd'hui, toutes les données sont récupérées par le nombre très important de capteurs présents sur les appareils. Doit-on considérer que ces données ne sont pas intéressantes, voire qu'il faut s'en débarrasser tels des déchets, ou bien, au contraire, part-on du principe que notre activité future consistera autant à fabriquer des avions qu'à savoir traiter ces données pour en extraire la valeur et pour nous améliorer ? Nos grands acteurs partagent-ils cette réflexion ou cherchent-ils à se débarrasser de ces données auprès d'autres acteurs ? Il ne s'agit plus seulement de questions de sécurité, mais véritablement de valeur. L'exemple le plus typique se situe dans le domaine de l'automobile. Certains fabriquent des voitures, tandis que d'autres font des Tesla. Une Tesla, c'est une voiture vendue à perte pour l'entreprise, du moins en apparence. Car il s'agit en fait d'un capteur géant. Ce qui fait la valeur d'une telle automobile, ce qui constitue le retour sur investissement, c'est justement la compilation des données qui n'appartiennent pas au conducteur mais à la marque. Ce modèle est perturbant dans la mesure où il se situe en dehors des paradigmes usuels. Mais les acteurs qui n'ont pas compris l'importance de la valeur des données sont en train de rater une opportunité et sont probablement voués à disparaître. L'évolution technologique impose aux acteurs de devenir des acteurs numériques au sens propre, pas seulement en tant que simples consommateurs.

M. Thomas Gassilloud, président et rapporteur. Les acteurs américains sont particulièrement doués pour convaincre les plus hauts niveaux de gouvernance et pour mettre à disposition gratuitement des ressources pendant plusieurs mois. Les décideurs sont par ailleurs un peu complexés de se porter sur des choix français, dans la mesure où, si finalement cela ne fonctionne pas, on leur reprochera sûrement d'avoir pris un tel risque. Notre rôle devrait peut-être consister à « dérisquer » le choix français.

M. Guillaume Poupard. C'est tout à fait vrai. C'est le biais classique de tout acheteur, qui opte pour le même produit que les autres, même si c'est moins bon et même si c'est plus cher. Avoir le courage de prendre une option différente constitue une vraie prise de risque. On constate exactement la même problématique s'agissant du choix entre les offres dominantes et les offres des acteurs émergents qui proposent de très bons produits. Ce courage ne peut pas reposer sur les seules épaules de l'acheteur. Cela doit entrer dans le cadre d'une politique impulsée par les décideurs. Il faut valoriser de genre de démarche, et je suis certain que l'on peut collectivement les y aider.

S'agissant du RRF, il me semble que s'appuyer sur les infrastructures civiles existantes pour le tout-venant est intelligent en termes d'optimisation, à la fois sur le plan des fonctionnalités et du coût. Mais il faut évidemment que ces infrastructures soient complétées par des « morceaux » de système qui assurent son bon fonctionnement. Le fait qu'il existe des morceaux non résilients dans les RRF, même majeurs, n'est pas forcément choquant. Par contre, il est indispensable de trouver des assemblages qui fonctionnent, qui soient moins onéreux et tout aussi résilients que la création d'un produit *ad hoc* qui serait forcément plus cher, plus fruste en termes de fonctionnalités, et qui pourrait s'avérer tout aussi décevant en cas de crise s'il était mal pensé.

La réunion se termine à dix heures cinq.

Membres présents ou excusés

Mission d'information sur la résilience nationale

Présent. - M. Thomas Gassilloud

Excusé. - M. Alexandre Freschi