ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Mercredi
22 septembre 2021
Séance de 15 heures

Compte rendu n° 19

SESSION EXTRAORDINAIRE DE 2021

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

ASSEMBLÉE NATIONALE

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

Mercredi 22 septembre 2021

La séance est ouverte à quinze heures

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

———

M. le président Alexandre Freschi. Nous abordons une série d'auditions et de tables rondes consacrées au risque cybernétique et à la cybersécurité, thème central pour notre réflexion sur la résilience. Je remercie M. Nadi Bou Hanna, directeur interministériel du numérique, d'avoir répondu à notre invitation pour ouvrir cette séquence. Nous attendons que cette audition nous donne une vision globale de la place croissante du numérique dans le fonctionnement de l'État et des collectivités, et qu'elle nous permette de prendre la mesure des menaces et attaques auxquelles la puissance publique est exposée dans l'espace cyber.

M. Nadi Bou Hanna, directeur interministériel du numérique (DINUM). Je commencerai par une présentation succincte des métiers de la DINUM pour mieux situer son rôle et sa complémentarité avec d'autres services de l'État, notamment avec l'agence nationale de sécurité des systèmes d'information (ANSSI).

La DINUM est placée sous l'autorité de Mme Amélie de Montchalin, ministre de la transformation et de la fonction publique. Elle conseille le Gouvernement en matière de stratégie du numérique, ainsi que les administrations pour ce qui relève de sa mise en œuvre. Si chaque ministère est autonome et dispose de sa propre stratégie en la matière, elle cherche essentiellement à mutualiser les actions et à développer une stratégie commune.

Elle assure également un rôle d'opérateur en matière de réseaux de télécommunications. La DINUM a notamment conçu et gère le réseau interministériel de l'État (RIE), couvrant 14 000 points de présence en France – essentiellement des sites administratifs – et leur permettant de bénéficier de services communs et d'une protection commune.

La DINUM se charge par ailleurs de la promotion des nouveaux usages, se démarquant en cela des autorités responsables de la sécurité. Elle est en quête d'un compromis permanent entre la satisfaction des utilisateurs – citoyens et agents publics –, l'innovation, le progrès et la sécurité. C'est notamment le cas pour le métier de la donnée, puisqu'elle doit à la fois protéger les données et faciliter leur utilisation et leur partage pour opérer de nouveaux services et garantir la transparence de l'action publique.

Son dernier métier, en lien avec le plan de relance, est celui de fonds d'investissement interne. En effet, la DINUM gère un fonds d'accélération de la transformation numérique qui soutient tous les ministères désireux de rattraper leur retard ou de prendre un temps d'avance sur leurs projets numériques.

Ces métiers sont encadrés par le décret n° 2019-1088 du 25 octobre 2019, qui définit le système d'information de l'État, les missions de la DINUM, mais aussi ce que devraient être les missions de chacune des directions du numérique des différents ministères.

La cybersécurité constitue quant à elle une composante essentielle de la politique du numérique, dont le chef de file reste l'ANSSI, avec laquelle nous collaborons étroitement pour définir et mettre en œuvre des objectifs communs et en contrôler l'application. À titre d'exemple, notre direction est en charge d'auditer tous les grands projets informatiques d'un coût supérieur à 9 millions d'euros pour s'assurer qu'ils demeurent sous contrôle et produisent les résultats escomptés dans les budgets et délais impartis, l'ANSSI s'assurant pour sa part que ces projets soient conformes et engagés dans le respect des enjeux de cybersécurité.

M. Thomas Gassilloud, rapporteur. En tant que directeur de la DINUM, comment percevez-vous cet enjeu de résilience nationale ? Quel est votre rôle pour atteindre un objectif de résilience nationale ?

M. Nadi Bou Hanna. Lorsque l'on parle de résilience, l'on pense tout de suite à la capacité de produire et opérer des solutions numériques et de maîtriser leur évolution dans le temps. À l'échelle française et européenne, dans le domaine des matériels – ordinateurs, smartphones – ou des systèmes d'exploitation, nous ne disposons d'aucun constructeur ou opérateur de taille significative. Sur les couches basses – matériels et logiciels d'opération – nous devons composer avec un état du marché qui n'est pas en prise directe avec les forces vives françaises ou européennes.

Pour autant, notre offre est suffisamment diversifiée et notre capacité d'innovation – en particulier dans le domaine logiciel – est suffisamment forte pour nuancer ce constat anxiogène initial. Durant la crise sanitaire, lorsque nous avons été contraints de changer le modèle de travail et d'assurer une continuité du service public *via* le travail à distance des agents, nous sommes parvenus à trouver des solutions sur le marché, avec le concours des personnels des différents ministères, dans un délai relativement court. Nous disposons donc, au sein des administrations et à l'échelle de la nation, d'un capital humain de qualité, qui permet de réagir aux crises et qui permettra de mieux s'y préparer, en inscrivant à l'agenda des administrations le sujet de la souveraineté numérique et de la résilience en situation de crise, avec l'objectif d'investir davantage que par le passé. Par exemple, le réseau interministériel de l'État opéré par notre direction a désormais vocation à accueillir les moyens de communication de crise de l'État, ce qui n'était auparavant pas le cas.

Nous sommes donc bien engagés dans une prise de conscience collective de cette nécessité d'investir dans les hommes, les systèmes, les réseaux et les procédures pour garantir une continuité d'activité. Malgré mon propos introductif anxiogène, je suis plutôt optimiste quant à la prise de conscience et à la capacité d' entreprendre de la nation.

M. Thomas Gassilloud, rapporteur. Sur la partie matérielle, nous raisonnons plutôt selon une logique de stocks et non de flux, puisque l'État dispose de stocks autonomes de matériels informatiques. De fait, si nous devions être confrontés à des difficultés d'approvisionnement, le fonctionnement hors maintenance de nos systèmes ne serait pas perturbé. Il n'y aurait pas d'atteinte immédiate à la résilience nationale. Néanmoins, il est important de rappeler notre dépendance matérielle aux pays tiers s'agissant de l'informatique du quotidien, sachant qu'Atos a développé, sous l'impulsion du commissariat à l'énergie atomique (CEA), des systèmes en propre pour le calcul de haute performance.

Notre mission d'information s'intéresse aux chocs de nature à perturber gravement le fonctionnement de la nation et de ses services vitaux. Pouvez-vous préciser la nature des 14 000 points raccordés au RIE et indiquer quels éléments – notamment la dépendance vis-à-

vis d'opérateurs tiers ou le fonctionnement d'internet au sens large – pourraient porter atteinte à son bon fonctionnement ?

M. Nadi Bou Hanna. Le stock auquel vous faites référence a été considérablement étendu durant les dix-huit derniers mois. Avant la crise sanitaire, l'État ne disposait que d'un stock de 100 000 ordinateurs portables dotés d'une capacité d'accès à distance au système. En juillet 2021, nous dépassions les 350 000 agents entièrement équipés pour travailler à distance. Les nouvelles formes de travail hybrides combinant présentiel et télétravail ont été ainsi rendues possibles par un effort de rattrapage conséquent, par la relève du niveau de stock et par le développement de nouvelles pratiques professionnelles.

S'agissant du RIE, deux volets sont à distinguer. Le premier concerne la capillarité du réseau et la possibilité d'atteindre des sites physiques. En la matière, le RIE couvre 14 000 sites administratifs en métropole et dans les territoires ultramarins, qui ont ainsi la possibilité d'accéder à différentes ressources – bases de données, sites d'information, logiciels – dans le cadre d'une bulle de confiance sécurisée et supervisée 24 heures sur 24. Bien entendu, ce réseau ne fonctionne pas en autarcie et a vocation à interagir avec le monde extérieur – entreprises, citoyens, partenaires tiers. À l'ancienne conception de la défense périmétrique s'est substitué un système reposant sur de nombreux échanges avec le monde de l'Internet, qui se sont évidemment intensifiés avec la généralisation du télétravail. Il s'agit donc d'un univers beaucoup plus composite que par le passé, ce qui permet de renforcer le niveau de résilience de l'État. En effet, en concentrant et en maîtrisant les points de sortie et les points d'échange, en y consacrant de l'expertise et des moyens techniques, nous pouvons améliorer le niveau de sécurité d'ensemble. Nos équipes assurent ainsi une gestion permanente du risque pour faciliter les échanges avec les tiers tout en contrôlant les flux.

Vous évoquiez le sujet de la dépendance aux opérateurs. Or le paradigme a également évolué dans ce domaine. Historiquement, nous avions tendance à confier nos réseaux à un opérateur de confiance. Aujourd'hui, pour diversifier le niveau de risque et en diluer la gravité, nos réseaux s'appuient sur des opérateurs multiples, tandis que nous avons parallèlement réinternalisé, au sein de l'État, la capacité d'animation de ces acteurs. S'il est vrai que nous sollicitons davantage de sous-traitants, nous réinternalisons également certaines fonctions critiques – architecture, reconfiguration du réseau en cas de crise, etc.

M. Thomas Gassilloud, rapporteur. Si je comprends bien, vous faites fonctionner le RIE en vous appuyant sur des liaisons fournies par des opérateurs privés, dont la diversité et les garanties contractuelles de temps de rétablissement vous permettent d'envisager sereinement le bon fonctionnement du réseau. Le problème est que ces garanties de temps de rétablissement excluent souvent les cas de force majeure, qui nous intéressent au premier chef. Typiquement, en cas de crise, les opérateurs pourraient rencontrer des difficultés à fonctionner, par exemple en cas de défaut de la cybersécurité. Je suppose donc que votre réseau couvre à la fois des sites sensibles que vous êtes en mesure d'interconnecter en maîtrisant vous-mêmes les couches basses et des sites moins sensibles pour lesquels vous vous contentez d'un simple cryptage pour sécuriser la connexion à internet et le télétravail. Pourriez-vous donc nous éclairer sur cette granularité et nous confirmer que vous assurez bien une maîtrise de bout en bout des sites les plus sensibles ? Par exemple, nos préfectures savent-elles communiquer avec l'échelon central national sans passer par des opérateurs tiers ? Ou ces opérateurs sont-ils nécessaires à la bonne communication avec ces préfectures ?

M. Nadi Bou Hanna. Durant les dix dernières années, la continuité de service du RIE a toujours été assurée, y compris lors du pic de la crise sanitaire. Cela passe

effectivement par une différenciation du niveau de sensibilité des sites et par une adaptation du réseau de collecte, qui repose sur des technologies diversifiées selon la sensibilité du site. Dans le cadre du RIE, une granularité suffisante est prévue pour garantir une diversification de technologies, d'opérateurs et de matériels pour les sites les plus sensibles qui, en cas de crise marquée, devront communiquer en toutes circonstances – préfectures ou autres. Nous pouvons notamment faire appel à des technologies intrusives sur les réseaux des opérateurs. Je pense notamment au réseau radio du futur, le futur réseau mobile de la police et de la gendarmerie, doté de capacités d'intrusion et de priorité sur les réseaux des opérateurs, qui offrira une bande passante et une connectique garanties sur l'ensemble du territoire national en cas de crise. Nous pouvons donc aller très loin dans ce traitement spécifique des sites les plus sensibles, puisqu'entre 1 500 et 2 000 sites auront vocation à bénéficier d'une résilience renforcée.

M. Thomas Gassilloud, rapporteur. En d'autres termes, la stratégie de résilience repose sur une diversification des opérateurs tiers et non plus sur une maîtrise de bout en bout des couches basses de ces réseaux. C'est précisément le mouvement que l'on observe dans différents services de l'État. Les gendarmes sont eux-mêmes en train de basculer de réseaux qu'ils maîtrisent en propre vers l'usage de radios de type 4G-5G reposant sur d'autres critères de résilience – autant les gendarmes sont assurés par la couverture de zone, autant un opérateur est davantage intéressé à la couverture de populations. Avez-vous imaginé, en matière de réseau, des cas critiques qui ne permettraient pas aux réseaux des opérateurs privés de fonctionner et de vous délivrer du service ? Avez-vous également songé à des alternatives hertziennes ou satellitaires pour continuer à communiquer avec des préfectures qui seraient coupées du monde ?

M. Nadi Bou Hanna. Le rôle de la DINUM est d'assurer l'équilibre entre le progrès, la réponse au service, la sécurité et la résilience. Dans la mesure où notre premier enjeu consiste à accompagner la transformation numérique des organisations et de leurs méthodes de travail *via* des services à valeur ajoutée et des bandes passantes accrues, nous ne pouvons pas nous satisfaire des moyens haute fréquence (HF) des années 80, qui ne sont absolument pas en capacité de véhiculer ce type de trafic. Si nous ne sommes pas en mesure d'apporter le service attendu, nous serons confrontés au développement du *Shadow IT*, de la débrouille, de l'usage de services gratuits sur internet, avec les enjeux de souveraineté et de protection des données que nous connaissons.

Pour relever ce défi, nous devons nous appuyer sur des industriels qui investissent considérablement en hommes, moyens, machines et ressources pour garantir un niveau élevé de service ; en complément, sur différentes stratégies pour apporter la protection, la résilience en situation de crise et la continuité d'activité en mode dégradé : protection, chiffrement, interception des menaces et des attaques ; diversification des opérateurs et gestion automatisée de la bascule. Cette stratégie permet clairement de combiner les deux objectifs, à savoir les services attendus et la résilience.

Vous m'interrogez sur les moyens de dernier recours, sujet sur lequel j'ai travaillé tout au long de ma carrière, en particulier pour les services de l'État à l'étranger. Nous disposons bien sûr d'une capacité de déploiement de bulles tactiques. En cas de crise majeure, l'appui sur le réseau radio du futur et les autres moyens de l'État – HF, satellitaire, etc. – font justement partie de la batterie de solutions que nous sommes capables de déployer pour assurer cette continuité de communication en situation de crise.

Mme Marine Brenier. Vous partez souvent du postulat qu'internet continuerait de fonctionner. Or la réflexion sur la résilience ne doit exclure aucun risque. Avant le passage à l'an 2000, on redoutait fortement un plantage massif de l'internet, alors même que nous n'en étions pas aussi dépendants qu'aujourd'hui. Votre direction serait-elle à même de faire face et de répondre à une panne massive du réseau internet consécutive à une cyberattaque terroriste ?

Vous parliez également des nouveaux réseaux déployés par la gendarmerie. Sur mon territoire, lors de la tempête Alex, les réseaux de voirie amenant la fibre dans les villages ont tous été coupés, privant les populations de tout accès à internet. Les communications avec les secours ont été complexifiées d'une manière démesurée, puisque nous ne parvenions pas à contacter les opérateurs sur place. Malgré les téléphones satellitaires détenus par certaines collectivités et la gendarmerie, il était très difficile d'entrer en communication avec les personnes sur place et d'organiser les secours. Votre direction a-t-elle travaillé sur un retour d'expérience à la suite de ce genre de situation ? Est-on à même de pouvoir répondre à ce genre de difficulté sur le territoire ?

M. Nadi Bou Hanna. La panne majeure d'internet est un scénario intégré aux stratégies de continuité d'activité et auquel nous devons nous préparer, en espérant qu'il ne se produira pas. D'une certaine manière, le RIE – qui interagit avec internet tout en s'appuyant sur des ressources spécifiques gérées par des opérateurs – constituerait une force si cet évènement devait se produire. Néanmoins, cela ne suffit pas, puisque de plus en plus d'applications informatiques reposant sur le *cloud* sont désormais utilisées pour faire fonctionner les services de l'État et pour permettre aux citoyens d'effectuer leurs démarches administratives ou de s'informer sur leurs droits à distance.

Dans ce contexte, le Premier ministre a diffusé une circulaire en date du 5 juillet pour inciter les administrations à se saisir des enjeux du *cloud* : informatique continue (*DevOps*), services locatifs sur étagère, etc. Tout l'enjeu consiste à assurer une continuité de service sur les applicatifs les plus critiques tout en protégeant les données des citoyens, des agents ou des entreprises. En l'occurrence, cette circulaire forge un compromis entre l'appui sur les services fournis par les acteurs industriels et commerciaux et la nécessité de maintenir, au sein de l'État, des compétences et des infrastructures pour accueillir des systèmes dits critiques.

Bien entendu, cela ne répondra pas à toutes les situations de crise possibles et imaginables. Mécaniquement, la section des câbles de fibre optique ou la rupture des antennes 4G-5G entraîne une rupture des possibilités de communication, si ce n'est les communications satellitaires, dont les débits sont limités et dont les déploiements ne sont pas à la portée du grand public. Nous avons la possibilité de déployer des bulles tactiques pour que les autorités et les forces d'intervention se coordonnent, mais elles n'assureront pas la continuité de communication pour tous les citoyens. Les réponses en situation de crise ne sauraient donc être que partielles pour garantir les communications les plus critiques.

Retenez toutefois que la stratégie d'ensemble de l'État en matière de numérique tient à la fois compte des besoins de continuité et de protection et des besoins d'apport de nouveaux services, en lien avec les exigences croissantes des usagers et des agents publics, qui ne doivent aucunement se sentir déclassés par rapport aux salariés du privé. Il nous faut trouver en permanence cet équilibre entre les opportunités et les menaces.

M. le président Alexandre Freschi. La quête d'équilibre entre innovation, progrès et sécurité est salutaire. L'actualité récente a montré que le QR code de vaccination du

Président de la République avait été diffusé et que des hôpitaux avaient été victimes de vols de données. Quel est notre degré de perméabilité par rapport aux cyberattaques ? Dans quelle mesure pouvez-vous garantir la protection des données est totale ?

M. Nadi Bou Hanna. Votre question dépasse mes prérogativesμ. Le directeur de l'ANSSI sera plus à même de répondre aux questions de cybersécurité et de protection contre les attaques. Je puis seulement souligner que les investissements sont mis en œuvre, en particulier au sein de l'État, afin de relever le niveau de protection, dans un contexte de course permanente entre les attaquants et les défenseurs et d'absence de risque zéro. De fait, c'est en continuant à investir dans les expertises et dans les outils techniques que nous parviendrons à mieux nous défendre face aux attaques.

En parallèle, la culture de la donnée me semble être un enjeu essentiel pour toutes les parties prenantes. Durant des années, nous avons été bercés par l'internet gratuit, les services prêts à l'emploi, sans accorder la moindre attention à la contrepartie de cette gratuité. Or la gratuité signifie que vous êtes vous-même le produit et que vous acceptez de transmettre vos données à des tiers qui sauront les monétiser ou les détourner. Il existe un véritable problème de prise de conscience collective du pouvoir des données et des enjeux parfois contradictoires qui y sont associés. Ma direction s'occupe notamment de la démarche *Dites-le-nous une fois*, qui vise à favoriser le partage en confiance de données entre administrations pour qu'un citoyen n'ait pas à fournir plusieurs fois les mêmes justificatifs.

En tout état de cause, nous pouvons espérer que les différents incidents impliquant la diffusion d'informations confidentielles sur internet contribuent à l'acculturation des décideurs et des citoyens au risque que constitue la mise à disposition de ses données personnelles. Nous voyons bien que les données doivent être protégées, puisque des agresseurs vont chercher à se les procurer à des fins peu recommandables. Une éducation collective me semble ainsi nécessaire, sans doute dès le plus jeune âge, étant entendu que les risques comportementaux peuvent difficilement être régulés. Je suis d'ailleurs horrifié de constater que de grands groupes comme Facebook envisagent de construire des solutions pour les jeunes de moins de 13 ans, qui ne sont pas encore acculturés au risque de la donnée.

Mme Marine Brenier. On nous explique souvent, s'agissant des dossiers de police, que les transferts de données personnelles entre services sont compliqués à cause du règlement général sur la protection des données (RGPD) et de la commission nationale de l'informatique et des libertés (CNIL). De la même manière, on sait que le dossier médical personnel numérique est compliqué à mettre en place en raison des contraintes pesant sur la communication des données personnelles des usagers. Existe-t-il des ouvertures législatives ou réglementaires facilitant ces transferts ?

M. Nadi Bou Hanna. Plusieurs textes encadrent le partage de données entre administrations et rendent possible leur transfert. La CNIL veille évidemment à ce que la finalité de ces données ne soit pas détournée, sachant que la France mise sur des approches ciblées pour pouvoir interconnecter certaines données. De fait, c'est bien le caractère explicite des finalités – que la CNIL contrôle – qui rend possible le partage des données. Hélas, les administrations utilisent parfois cet argument pour ne pas pousser la logique du partage des données jusqu'à son terme, ou comme un frein à la simplification. Pour travailler régulièrement avec les services de la CNIL, je puis confirmer que son intention est beaucoup plus mesurée : dès lors que la finalité est claire et encadrée, le partage des données est possible. Je suis moins compétent sur la question des données de santé, mais je ne suis pas certain que les difficultés soient liées à l'impossibilité juridique de partage des données.

Mme Sereine Mauborgne. La semaine dernière, plusieurs préconisations ont été émises dans le cadre du forum international de la cybersécurité (FIC) : approfondir la boîte à outils cyberdiplomatique européenne ; enrichir les outils de demande d'information et d'action corrective ; dresser une liste noire des entreprises ayant vendu des entités à certains régimes ; rendre opérationnelle la clause de défense mutuelle des États membres. Quel est votre avis sur la question ?

M. Nadi Bou Hanna. Ces champs sont trop éloignés de mon domaine d'intervention pour que je puisse vous répondre.

M. Thomas Gassilloud, rapporteur. Je demandais récemment à un expert de m'expliquer pourquoi les patrouilles de police américaines se rendaient parfois sur site avec seulement une ou deux personnes, contrairement à ce que l'on peut observer chez nous. Une partie de la réponse réside dans une meilleure connaissance – du fait d'un partage de données plus élargi – des zones d'intervention, qui permet de mieux dimensionner les forces en présence. En France, les forces de l'ordre ont récemment essuyé des tirs dans le cadre de plusieurs interventions parce que les données liées à la détention d'armes – notamment dans les milieux survivalistes – n'avaient pas été portées à leur connaissance. J'ai bien noté que la CNIL n'était pas nécessairement l'élément bloquant, mais la mise à disposition des données pourrait encore s'améliorer pour que nos forces de l'ordre sachent où elles mettent les pieds.

Pour en revenir à la résilience des réseaux, avez-vous une estimation du nombre de bulles tactiques dont nous disposons, sachant que ces bulles n'apportent qu'une solution de contournement localisée lorsque le réseau primaire est hors service ?

Plus globalement, je m'interroge sur l'indépendance vis-à-vis d'internet. Au niveau géopolitique, tous les grands compétiteurs stratégiques mondiaux se préoccupent de l'indépendance de leurs réseaux internet : les Chinois, pour une raison de maîtrise de l'information, mais aussi de résilience ; les Russes ; la question ne se pose pas dans les mêmes termes pour les Américains, puisqu'ils détiennent les clés d'internet pour les sujets de gouvernance, de serveurs, etc. ; les Anglais ne se posent pas non plus la question, puisque leur dépendance aux Américains ne leur pose aucune difficulté. En tout cas, j'ai l'impression que la France – et plus globalement la plaque européenne – est le seul membre du conseil de sécurité de l'Organisation des Nations unies (ONU) qui s'expose à une faiblesse dans ce domaine.

Dans ce contexte, comment évaluez-vous le degré de fonctionnement des opérateurs télécom sans internet ? Le réseau mobile français et vos interconnexions dans le cadre du RIE peuvent-ils fonctionner sans internet ? Ne pensez-vous pas que, pour être véritablement résilients, nous devrions nous interroger sur la maîtrise du fonctionnement d'internet, à l'instar des réflexions menées à Pékin comme à Moscou ? Si nous devions un jour nous confronter à ces acteurs, nous serions sans doute moins en capacité de perturber leurs réseaux que l'inverse.

M. Nadi Bou Hanna. Je ne suis pas en mesure de vous répondre sur la question des bulles tactiques. Le ministère de l'intérieur dispose de chiffres plus actualisés concernant la capacité de projection de ces bulles sur le territoire national. En tout état de cause, le réseau radio du futur n'en est qu'au début de sa construction et de sa mise en œuvre.

Concernant internet, je rappelle que la DINUM s'intéresse principalement à son impact sur les services de l'État, et non sur l'économie française et la vie quotidienne des

ménages. Il conviendrait plutôt d'interroger la direction générale des entreprises – dépendant du ministère de l'économie et des finances – pour disposer d'une vision plus précise de ce niveau de risque. Pour ma part, j'apporterai quelques éléments permettant d'alimenter votre réflexion.

Dans le cadre de notre RIE, nous avons fait en sorte de pouvoir fonctionner indépendamment d'internet. Dans cette configuration, le travail à distance est par définition impossible. Nous disposons toutefois d'une réelle capacité de travail et de continuité d'activité. Durant la crise sanitaire, la question se posait de savoir si les fournisseurs de logiciels non européens n'accorderaient pas une préférence de transit et de trafic aux entreprises et ressortissants de ces pays non européens. Pour limiter ce risque, nous avons décidé de nous appuyer sur un écosystème de partenaires français et européens. À titre d'exemple, nous avons déployé la messagerie instantanée Tchap, qui couvre aujourd'hui 250 000 agents de l'État, ainsi que des parlementaires. Ce service reposant sur un logiciel en code ouvert édité par une PME franco-anglaise est autonome de tout interventionnisme d'acteurs extérieurs à l'État. Il en va de même pour les outils collaboratifs de partage de documents entre agents publics, puisque nous avons travaillé avec deux PME françaises pour construire une plateforme désormais utilisée par plus de 170 000 agents publics. La même question s'est posée pour les systèmes de visioconférence, et nous avons préféré investir sur le logiciel libre et sur l'opération de systèmes garantissant la non-interception des communications et la résilience en cas de saturation.

Ainsi, même si je ne réponds pas directement à votre question, je puis vous confirmer que l'État continuerait à fonctionner même en cas de crise grave d'internet. Les moyens que nous avons mis en place sont étanches non seulement aux technologies et aux opérateurs d'internet, mais aussi aux grands fournisseurs de logiciels et opérateurs de c*loud*. Bien évidemment, si internet tombait, l'impact serait surtout désastreux pour les citoyens et les entreprises, mais je crois savoir que d'autres entités de l'État travaillent sur ces questions.

M. Thomas Gassilloud, rapporteur. Dans la mesure où le RIE dépend d'opérateurs télécom, êtes-vous certains que ces derniers savent fonctionner sans internet ? Les centres de gestion des incidents des opérateurs s'appuient sur de nombreuses applications en mode web. Je ne suis donc pas persuadé que les opérateurs savent fonctionner sans internet.

Peut-on par ailleurs concevoir, compte tenu de la vitalité des usages de l'internet, notamment dans le domaine de la santé, une dépendance stratégique majeure à ce sujet, alors que notre pays a toujours cherché à se prémunir des grandes dépendances stratégiques et qu'une seule dépendance suffit pour créer un problème de résilience ?

M. Nadi Bou Hanna. Au-delà de la périphérie de l'État, le service public est évidemment assuré par les collectivités territoriales, les hôpitaux, les universités, des opérateurs. Ceux-ci ne relèvent pas directement du champ d'intervention de l'État. Pour autant, nos stratégies numériques intègrent la mise en place de lieux de partage des bonnes pratiques, de recommandations, etc. La stratégie *Cloud au centre* publiée le 1er juillet par le Premier ministre concerne les services de l'État au premier chef, mais nous serions ravis que les autres partenaires du service public se saisissent de ces considérations de protection tout en proposant de nouveaux usages attendus par les citoyens.

Si l'idée d'un internet français étanche au reste d'Internet peut sembler séduisante en théorie, sa mise en place semble tout à fait illusoire, puisqu'elle nécessiterait des investissements colossaux, sans compter que la richesse d'internet repose justement sur la

possibilité d'accéder à des ressources localisées hors du territoire national. À défaut d'être empêchée, la compromission globale d'internet peut être rendue complexe par l'éparpillement des nœuds de réseau aux quatre coins du globe, même si un nombre limité d'acteurs occupe une place prépondérante dans le fonctionnement de ce réseau. En cas de crise majeure, l'État devra surtout continuer à assurer un service public, y compris en mode plus ou moins dégradé. Pour les autres incidences, il convient nécessairement d'imaginer des stratégies de repli. Je suppose que des cellules du ministère de l'économie et des finances travaillent sur ce scénario.

M. Thomas Gassilloud, rapporteur. Je note que votre réponse n'est pas affirmative sur la garantie de fonctionnement du RIE sans internet. Il serait donc intéressant d'imaginer un crash-test au cas où internet était coupé à la suite d'un incident technologique. Si les marines de guerre référencent aujourd'hui des câbles sous-marins, c'est bien parce que nous évoluons dans un monde en compétition au sein duquel des adversaires stratégiques peuvent déployer des menaces hybrides. Mon idée n'est certainement pas l'autonomie d'un réseau internet européen, mais la maîtrise des dommages engendrés par la rupture d'un câble sous-marin ou l'action d'un État tiers. Qui aurait pu, il y a deux ans, imaginer une fermeture des frontières – que l'on pensait devenues obsolètes – entre la France et l'Allemagne ? Nous savons à présent que les frontières peuvent être rapidement rétablies. Ne devrait-on donc pas anticiper ces scénarios, sachant que d'autres acteurs internationaux ne s'en privent pas ? Il me semble que cette question de la capacité à faire fonctionner notre réseau internet avec de nombreux services dégradés mérite d'être posée, en complément de la question du risque cyber, laquelle suppose un bon fonctionnement du réseau.

Pouvez-vous par ailleurs nous renseigner sur le contrôle des autorités américaines sur le fonctionnement d'internet ? Les Américains – qui assurent largement la gouvernance d'internet – auraient-ils la possibilité de couper, d'un clic, l'internet français ?

M. Nadi Bou Hanna. Le risque de panne d'internet chez les opérateurs sur lesquels nous nous appuyons est identifié, sans que nous soyons en mesure de l'objectiver. Néanmoins, nous prenons nos dispositions pour être capables de reconfigurer nos réseaux au cas où les opérateurs deviendraient défaillants. Dans le schéma stratégique du RIE que je mets en place au sein de notre direction, nous prévoyons cette reprise en main de la capacité de reconfiguration des nœuds critiques que sont les routeurs, ce qui réduit notre dépendance aux opérateurs si ceux-ci devenaient défaillants. De même, la multiplication des opérateurs contribue à la réduction du risque global, sachant toutefois qu'aucune solution miracle n'a été identifiée au cas où tous les opérateurs seraient concomitamment compromis.

Plus généralement, je tiens à rappeler que les plans de continuité ou de reprise de l'activité constituent une obligation dans le domaine informatique. Il ne s'agit pas seulement de contribuer à l'effort documentaire. Récemment, à la suite de la panne d'un serveur informatique dans l'Est de la France, les services concernés ont immédiatement basculé sur un plan de continuité de l'activité. Si vous vous êtes suffisamment préparés à la crise, vous parvenez plus ou moins à en réguler l'impact lorsqu'elle survient.

Concernant enfin votre dernière question sur la capacité des Américains à couper l'internet en France, je ne dispose malheureusement d'aucune information à ce sujet.

M. le président Alexandre Freschi. Durant la crise sanitaire, l'État a choisi de travailler avec le service Doctolib. Pouvez-vous expliquer l'origine de cette décision ? Comment l'État a-t-il fait confiance à Doctolib ?

M. Nadi Bou Hanna. Cette décision relevait du ministère de la santé, sans intervention de notre direction. En tant qu'utilisateur, *a posteriori*, elle s'avère pertinente au regard de son impact positif sur la vaccination de la population. Les acteurs de la protection des données personnelles sont suffisamment pris en considération en France pour considérer que les données transitant par Doctolib n'ont pas été détournées de leur finalité.

M. Buon Tan. Dans l'hypothèse où un câble sous-marin serait sectionné ou saboté, nous pourrions nous appuyer sur les transmissions satellitaires. Quelles capacités ces transmissions peuvent-elles supporter ? Par ailleurs, disposons-nous de capacités suffisantes en France ou devons-nous également compter sur des moyens européens et/ou américains ?

M. Nadi Bou Hanna. Le sujet du *backbone* – le squelette des réseaux de communication – est évidemment suivi de près au sein de ma direction. Nous y consacrons d'importants investissements, que le plan de relance viendra soutenir, afin de disposer d'acheminements multiples en cas de compromission d'un point. Nous rencontrons parfois ce cas de figure lorsque des artères numériques sont tranchées par des travaux de voirie. Dans ce domaine, il est également important de nous appuyer sur des opérateurs différents et des technologies variées, car l'utilisation d'une technologie ou d'un matériel unique par plusieurs opérateurs constitue une faille. Ce panachage réduit le niveau de risque, sans toutefois le neutraliser puisque le risque zéro n'existe pas. L'important est que nous soyons capables de reconfigurer les réseaux à la volée, grâce à des agents disponibles 24 heures sur 24. Jusqu'à présent, nous avons échappé à des coupures complètes sur des artères principales, même si nous n'avons pas échappé à des pannes localisées. En tout état de cause, les sites critiques de l'État sont pourvus d'une redondance d'électricité, de câbles et d'opérateurs pour atteindre une résilience maximale.

M. Buon Tan. Ma question portait surtout sur les transmissions intercontinentales. Comment s'organiserait la communication entre continents en cas de coupure de câbles sous-marins ?

M. Nadi Bou Hanna. Je m'occupais auparavant des télécommunications du Quai d'Orsay, où ces sujets de gestion de crise et de communications à longue distance sont critiques. Depuis, la capacité satellitaire a été réduite, car il était difficile de maintenir une bande passante volumétrique sur l'intercontinental. Dans le même temps, nous assistons à un déploiement sans précédent de constellations bas débit et d'offres de communication satellitaire, accompagnées d'investissements massifs. Comment intégrons-nous cette capacité à notre pilotage global de réseau ? Logiquement, nous devons concevoir notre réseau radio du futur avec des offres satellitaires. Celles-ci ne sont pas encore arrivées à maturité, mais la capacité satellitaire fait bien partie du plan de montée en résilience, de même que la disponibilité de capacités reposant sur des constellations à bas débit et à faible temps de latence. Si un câble sous-marin devait être coupé entre les territoires ultramarins et la métropole, nous devrions être capables de basculer sur une autre liaison ou sur une liaison satellitaire.

M. le président Alexandre Freschi. Quelles sont les administrations le plus souvent ciblées par les tentatives de piratage de données ? Qui en sont les acteurs et où sont-ils localisés ?

M. Nadi Bou Hanna. Les attaques sont relativement nombreuses, à hauteur d'une attaque majeure – eu égard au volume de données échangées – par semaine sur les sites de l'État. Fort heureusement, ces attaques en déni de service – *Distributed Denial of Service,*

DdoS – sont arrêtées avant de franchir les portes du RIE et d'atteindre les sites. Certaines cibles sont malgré tout atteintes, puisque la presse s'est fait l'écho, ces derniers mois, de différentes attaques affectant les collectivités locales et les hôpitaux. Pour le moment, les attaques que nous interceptons sont contingentées. Je ne saurais caractériser l'objectif réel des attaquants, puisque nous faisons en sorte d'éviter cette extrémité et d'intercepter systématiquement les attaques en amont, avec des tentatives plutôt concluantes.

M. le président Alexandre Freschi. Quelle est la provenance de ces attaques ?

M. Nadi Bou Hanna. Je ne suis pas en mesure de vous répondre, notamment parce qu'il est très facile d'en masquer la provenance, ne serait-ce que par le recours à des objets connectés peu protégés. En tout état de cause, l'identification de la provenance des attaquants nécessite des investigations relevant plutôt de la défense que de la DINUM.

M. Thomas Gassilloud, rapporteur. Il me semble que, dans notre doctrine, l'attribution relève d'un acte politique, au-delà de la détection technique. Personnellement, j'ai plutôt confiance dans notre réponse nationale en matière de résilience cyber. Néanmoins, notre pays est particulièrement exposé. Sachant qu'il s'est toujours soucié de son autonomie sur divers sujets – notamment en matière énergétique, je suis convaincu qu'il doit afficher une ambition d'autonomie cyber en cohérence avec son histoire et ses responsabilités.

Je souhaite également vous interroger sur les usages et les applications. Pourriez-vous donner quelques exemples d'applications développées à la DINUM ? Lorsque vous les concevez, réfléchissez-vous d'emblée à un mode opératoire dégradé pour acquérir une résilience "*by design*" ?

M. Nadi Bou Hanna. Avant de répondre à votre question, je veux insister sur un point critique, celui des ressources humaines et de la disponibilité des talents. Derrière les enjeux de résilience, de souveraineté numérique ou d'innovation se trouve l'enjeu majeur de la capacité à disposer de profils dotés d'expertises solides qu'ils peuvent actualiser au fil du temps. À défaut, nous n'aurons d'autres choix que de nous appuyer sur des ressources extérieures non européennes. De mon point de vue, c'est l'enjeu majeur auquel nous sommes aujourd'hui confrontés : l'attractivité de l'État employeur pour les profils numériques. Comment faire en sorte que les ingénieurs experts sortant d'écoles ou d'universités aient envie de participer à ce service d'intérêt général qu'est la résilience numérique nationale ? Bien entendu, cet enjeu politique dépasse très largement mes prérogatives. Néanmoins, il est crucial d'inciter les étudiants à développer leur expertise numérique afin de disposer d'un vivier suffisamment important – en qualité et en nombre – pour aider les administrations, les entreprises, les opérateurs d'importance vitale à se confronter aux menaces et à saisir les opportunités propres à ce domaine. Notre réseau éducatif est malheureusement limité dans sa capacité à produire des talents en nombre suffisant, comme nous l'observons d'ailleurs dans d'autres pays européens. Si l'on doit s'attaquer au nœud du problème, répondre à cet enjeu s'avère essentiel pour améliorer notre résilience.

Pour en revenir à votre question sur les services que nous déployons, j'ai déjà parlé du RIE et de la messagerie instantanée Tchap, qui trouve son public plus rapidement que nous ne l'aurions pensé. Nous travaillons aussi avec la sphère sociale et les collectivités locales pour leur faire bénéficier de différents services. Nous avons ainsi lancé une plateforme d'audioconférence afin que n'importe quel agent ait la possibilité de réserver un pont sans passer par un dispositif organisationnel complexe. De même, tout agent pourvu d'une caméra doit pouvoir se connecter à un service de visioconférence pour échanger avec le plus grand

nombre. Il s'agit de services que nous construisons généralement en partenariat avec des entreprises de confiance, et que nous opérons nous-mêmes par la suite. Nous allons poursuivre cette initiative *via* le sac à dos numérique de l'agent public (SNAP), qui bénéficie d'un financement dans le cadre du plan de relance, afin de démocratiser l'accès à des services numériques de qualité pour tous les agents publics. Enfin, pour être complet, j'évoquerai aussi France Connect, désormais utilisé par plus de 30 millions de Français, et que les collectivités territoriales sont incitées à déployer sur leurs sites municipaux ou de petite enfance.

M. Thomas Gassilloud, rapporteur. Quelle serait l'opportunité de dupliquer l'approche RIE au périmètre national ou européen, étant entendu que tout devient désormais sensible, au-delà de la seule communication de l'État ? Nous sommes tous confrontés à des risques de cybersécurité, qu'il s'agisse des centres de décision, des centres militaires, des entreprises, des citoyens. En tout état de cause, même si l'idée paraît aujourd'hui saugrenue, j'ai la conviction que l'extension de l'approche RIE s'installera naturellement.

De la même manière, que penseriez-vous de l'extension du logiciel de messagerie instantanée Tchap à tous les citoyens, sachant qu'ils utilisent aujourd'hui WhatsApp, Telegram ou Zoom et sont écoutés par nos amis américains, russes ou chinois, avec un pillage systématique de nos données ? Vous faisiez précédemment référence au *Shadow IT*, mais nous savons justement que certains services importants de l'État s'organisent sur WhatsApp ou sur Telegram, y compris au sein d'administrations sensibles. Pourrions-nous donc envisager une extension de Tchap à l'ensemble du périmètre national ? La puissance publique dispose de leviers importants pour développer et promouvoir un WhatsApp français, ne serait-ce que par le biais du service national universel (SNU). Au-delà de la communication personnelle, nous pourrions tout aussi bien imaginer des cas d'usage d'interface avec les pouvoirs publics qui renforceraient l'attractivité de cette application, tout en garantissant l'absence de surveillance généralisée par l'État.

In fine, combien d'utilisateurs dénombrez-vous actuellement sur le service Tchap et combien cela coûte-t-il ? D'après ces chiffres, quel serait le montant d'un investissement visant à l'élargir au périmètre national ?

M. Nadi Bou Hanna. Tout le monde dispose aujourd'hui d'un ordinateur dans sa poche. Pour notre part, nous travaillons sur des services performants, de qualité et économiques. Vous ne convainquez pas les utilisateurs par la contrainte, mais parce que le service est réputé bon et facile à utiliser. En l'occurrence, Tchap a été pensé et conçu de cette manière, puisque les agents de l'État n'ont jamais reçu pour consigne de l'utiliser. Il ne s'agit d'ailleurs pas d'un service privé, mais d'un service de l'État, puisque nous nous sommes appuyés sur un logiciel en code libre développé par une entreprise avant d'internaliser la technologie et de la déployer sur les serveurs de l'État, avec l'appui de prestataires.

Maintenant, doit-on considérer que la messagerie instantanée est un service public à fournir au citoyen ? Je pense personnellement que c'est le cas, d'autant que Tchap a prouvé sa valeur auprès d'un panel de 250 000 agents non soumis à la contrainte, qui profitent désormais d'un moyen de communication en temps réel chiffré de bout en bout. Il existe donc bien un plan de croissance de ce service, qui pourrait devenir un service public. Du point de vue de l'ingénieur que je suis, ce produit a le potentiel pour rendre ce service. Est-il politiquement souhaitable que l'État opère la messagerie instantanée de tous les Français ? Eu égard aux enjeux de protection des libertés personnelles, je doute qu'il s'agisse de la bonne réponse à apporter. Sans doute s'agit-il d'une meilleure solution qu'un service proposé par des entreprises privées dont le modèle économique repose sur la valorisation de la donnée.

Est-ce pour autant un modèle acceptable à l'échelle nationale ? Il appartient au Parlement de se saisir de ce sujet.

M. Buon Tan. Est-il prévu de partager le système de messagerie Tchap avec d'autres partenaires européens ? Savez-vous si d'autres pays européens ont mis en place des dispositifs de ce type ? Après le RGPD, existe-t-il de nouvelles réflexions communautaires relatives à la protection et au partage des données ?

M. Nadi Bou Hanna. J'ai oublié de préciser que le coût unitaire de Tchap était inférieur à cinq euros par an et par utilisateur, et qu'il sera naturellement tiré à la baisse avec une base d'utilisateurs accrue. Déjà, quelques collectivités territoriales nous ont demandé de pouvoir accéder à Tchap, de même que des hôpitaux et l'assurance maladie, qui considèrent préférable d'utiliser ce dispositif plutôt que Telegram, Signal ou WhatsApp. Au niveau européen, plusieurs États membres nous ont demandé de leur présenter ce dispositif, qui devrait faire partie des pistes potentielles de coopération européenne. J'espère donc que d'autres partenaires européens proposeront de participer à l'émergence de ce service.

M. Thomas Gassilloud, rapporteur. Je suis ravi d'entendre un responsable opérant des services publics pour le compte de l'État affirmer que cette mission pourrait être étendue auprès du grand public. Reste à savoir si le jeu en vaut la chandelle, notamment du point de vue financier, sachant qu'il pourrait être tout aussi intéressant, à défaut d'implication directe des pouvoirs publics, d'inciter une entreprise française ou européenne à développer son propre logiciel de messagerie instantanée pour conquérir le monde.

La réunion se termine à seize heures trente.

Membres présents ou excusés

Mission d'information sur la résilience nationale

Présents. - Mme Marine Brenier, M. Alexandre Freschi, M. Thomas Gassilloud, Mme Sereine Mauborgne, M. Buon Tan