ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Jeudi
8 avril 2021
Séance de 11 heures

Compte rendu n° 56

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, *rapporteur*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Guillaume Vassault-Houlière, président-directeur général et cofondateur, et Mme Rayna Stamboliyska, vice-présidente en charge des affaires publiques et institutionnelles, de Yes We Hack

La séance est ouverte à 11 heures.

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons aujourd'hui M. Guillaume Vassault-Houlière, président-directeur général et cofondateur, et Mme Rayna Stamboliyska, vice-présidente de la gouvernance et des affaires publiques, de Yes We Hack.

Yes We Hack est une plateforme de mise en relation d'entreprises avec des hackers éthiques, créée en 2013. Spécialiste de la prime aux bogues (ou *bug bounty*), c'est-à-dire la chasse aux vulnérabilités, elle regroupe la première communauté européenne d'experts en cybersécurité.

Le gouvernement a récemment fait appel à Yes We Hack préalablement au lancement de l'application TousAntiCovid, qui portait à l'origine le nom de StopCovid.

J'aimerais que vous nous présentiez Yes We Hack, son actualité, son mode de fonctionnement, son processus de sélection de *hackers* et ses relations avec sa clientèle d'entreprises. Entretenez-vous des relations commerciales régulières avec des acteurs publics tels que l'État, les collectivités territoriales ou les hôpitaux ? Comment appréhendent-ils les enjeux de sécurité numérique et leurs solutions ? Manifestent-ils de l'intérêt pour le type d'offres que vous proposez ?

Je souhaiterais ensuite prendre du champ par rapport à la cybersécurité proprement dite. Le gouvernement prévoit d'y consacrer des moyens renforcés dans sa stratégie nationale « cyber ». Comment percevez-vous l'action des pouvoirs publics dans ce domaine ? Que pensez-vous des initiatives européennes, et notamment de la stratégie « cyber » présentée par la Commission européenne, ou encore de la révision envisagée de la directive *Network and Information System Security (NIS)* ?

À l'approche de la présidence française de l'Union européenne, à compter du 1er janvier 2022, il me semble important d'avoir les idées claires sur les priorités à défendre en la matière.

Quant à la diffusion d'une culture cyber au sein de la société, quel regard portez-vous sur le niveau de sensibilisation, aussi bien des entreprises et des administrations publiques, dont les collectivités territoriales, que des citoyens ? J'aimerais en outre aborder la formation aux compétences cyber, alors même qu'un campus cyber s'apprête à voir le jour avec l'appui, entre autres, de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Comment la France se positionne-t-elle par rapport à ces enjeux, comparée à d'autres pays ? Devrions-nous compléter notre offre de formation dans certains segments en particulier ? Nous resterait-il d'éventuelles lacunes à combler ?

M. Guillaume Vassault-Houlière, président-directeur général et cofondateur de Yes We Hack. Je reviendrai sur l'identité de Yes We Hack, sa coopération avec les ministères et institutions publiques, son vécu de la crise sanitaire et les moyens par lesquels nous incitons à la mise en place d'une cybersécurité efficace à l'échelle nationale, en

démystifiant les pirates ou *hackers*, en réalité des passionnés d'informatique d'une grande compétence ne demandant qu'à contribuer à l'amélioration de la cybersécurité.

Yes We Hack se présente aujourd'hui comme la première plateforme de *bug bounty* d'Europe. Nous fédérons 22 000 hackers présents dans 168 pays, ce qui nous permet de traiter les demandes de clients de tous types dans une trentaine de pays. Parmi notre clientèle figurent des entreprises connues comme BlaBlaCar ou Deezer et d'importantes banques asiatiques. Je ne suis bien sûr pas autorisé à toutes vous les citer. Nous disposons de bureaux en Suisse, à Munich et à Singapour.

Surtout présents en Europe et en Asie, nous employons près de cinquante personnes dans le monde entier, dont 40 % de femmes : une proportion dont nous sommes très fiers. Forte de sa croissance à trois chiffres et de sa capacité à exporter ses activités, notre *start-up*, qui ne mérite de fait peut-être plus cette dénomination, dispose d'une excellente résilience opérationnelle grâce à la diversité de notre communauté, en mesure de communiquer dans une multiplicité de langues et de se confronter aux technologies les plus diverses.

Nos clients font d'abord appel à nous pour tester des applications web ou mobiles du quotidien, quoique les demandes relatives aux objets connectés et aux voitures autonomes aient explosé. La mise en évidence de failles de sécurité à l'intérieur des périmètres soumis à nos tests donne lieu au versement de primes s'échelonnant de 50 à 15 000 euros, selon la criticité du bogue, une fois celui-ci validé par nos propres services ou par nos clients, selon la prestation pour laquelle ils optent.

Notre stratégie à l'international se consolide peu à peu. Il convient de le souligner. Nos effectifs devraient atteindre une centaine de personnes d'ici la fin de l'année, conformément à notre volonté d'accélérer notre développement. Cinq plateformes, essentiellement américaines, dominent aujourd'hui le marché de la chasse aux bogues. Nous avons la chance qu'existe en Europe une plateforme comme Yes We Hack. Nous ambitionnons de nous hisser, pas à pas, parmi le peloton de tête.

Nous avons travaillé sur StopCovid mais aussi sur la messagerie interministérielle Tchap pour améliorer sa transparence et sa fiabilité. Notre modèle, d'une grande agilité et d'une remarquable efficacité, apparaît parfaitement adapté au monde actuel. On dénombre environ quatre millions de postes en cybersécurité non pourvus à l'échelle de la planète. Nous sommes en mesure de mettre à pied d'œuvre jusqu'à des milliers de chercheurs pour qu'ils procèdent à des tests sur des applications en continu.

Chacun sait que les systèmes d'information actuels ne sont plus figés. Il arrive que les mises en production suivent une cadence horaire plutôt qu'annuelle comme jadis. Nous travaillons aussi bien avec des banques ou des assureurs que des acteurs numériques impliqués dans la défense ou encore des concepteurs d'objets connectés.

Un besoin de transparence et de confiance se fait jour chez les citoyens et les entreprises, et pas seulement en France. La cybersécurité constitue un outil de marketing. Il ne faudrait pas que son coût rebute, vu qu'elle assure une formidable impulsion aux affaires. En tant que Français, en tant qu'Européens, nous défendons des valeurs démocratiques, en matière de souveraineté et de données notamment, qui s'exportent à merveille. Le succès de notre plateforme en apporte la preuve. L'expertise et la qualité opérationnelle de Yes We Hack bénéficient aujourd'hui d'une reconnaissance mondiale. Nous poussons d'ailleurs nos clients à relayer notre promotion.

Parrot nous a récemment accordé sa confiance pour que nous assurions la sécurité de ses données et la transparence de son code. De plus en plus de gouvernements comprennent que notre communauté de *hackers*, autrement dit de passionnés, se définit, selon le *manifeste du hacker* publié en 1986, par l'envie d'apprendre et de se remettre en cause, soi et son environnement, afin d'améliorer celui-ci par souci du bien commun.

Nous avons transposé ces valeurs à l'échelle industrielle partout dans le monde et en tirons une immense fierté. Un nombre croissant d'États s'efforce de protéger notre communauté, comme le montrent bien certains rapports de l'organisation de coopération et de développement économiques (OCDE). Nous souhaitons qu'on lui donne les moyens de s'exprimer et d'étendre sa philosophie de vie à tous les domaines du quotidien pour améliorer celui-ci en lui apportant plus de transparence.

La traçabilité de l'argent joue un rôle notable dans notre sélection des *hackers*. Les primes leur sont versées par un prestataire bancaire, dans le respect des normes de lutte contre le terrorisme et le blanchiment d'argent, ce qui nous différencie d'ailleurs de nos homologues américains, au même titre que le Règlement général sur la protection des données (RGPD). Yes We Hack utilise aujourd'hui dans ses infrastructures des technologies européennes. Nous prônons notre savoir-être européen avec succès jusqu'aux États-Unis.

La prise de conscience de l'importance de la cybersécurité en France assure notre développement à l'échelle nationale. Nous améliorons la sécurité des outils numériques du quotidien qui gèrent des quantités de données, à la demande de nos clients, quels qu'ils soient. Nous répondons d'ailleurs à leurs demandes avec un égal sérieux, indépendamment de leur taille. Au final, tout le monde y gagne, les entreprises autant que les citoyens. Yes We Hack allie aujourd'hui une excellente qualité de service à une redoutable rapidité d'exécution.

Mme Rayna Stamboliyska, vice-présidente en charge des affaires publiques et institutionnelles de Yes We Hack. Les enjeux éminemment complexes et passionnants que vous avez esquissés dans votre introduction, M. le rapporteur, évoluent très rapidement. Ces derniers mois, de nombreux sujets sont revenus sur le devant de la scène, sous un éclairage différent d'il y a quelques années.

J'aimerais mettre en correspondance la vaste question de la définition de la souveraineté numérique avec la notion d'autonomie stratégique. Je me permettrai un trait d'esprit en vous annonçant que : « je suis venue vous parler d'Europe », à l'instar du président de la République en ouverture de son discours de la Sorbonne, voici quelques années. La souveraineté numérique française se joue aujourd'hui à l'échelle européenne et s'inscrit pleinement, selon notre point de vue, dans une démarche et une volonté d'autonomie stratégique européenne. Bien sûr, cette dernière notion évolue extrêmement vite.

Je me rappelle que les débats sur la souveraineté numérique tournaient, voici une dizaine d'années, autour de la gouvernance d'Internet. Une fracture se dessinait alors entre les approches technicistes occidentales et des conceptions plus centrées sur l'accès à l'information à l'Est. L'accès à la connaissance et à la liberté d'expression permises par le numérique sont ensuite revenues sur le devant de la scène, avant de céder la place aux préoccupations de surveillance liées aux révélations d'Edward Snowden en 2013 et 2014. Depuis, nous avons vécu, ou plutôt, survécu à la présidence de Donald Trump, durant laquelle se sont cristallisées des tensions géopolitiques d'une importance cruciale autour de questions d'économie stratégique, notamment sous son versant technologique. Le mandat de Donald Trump a donné un coup d'arrêt à un multilatéralisme que l'on croyait acquis, encore que la

situation semble se débloquer dernièrement, depuis le changement d'équipe au pouvoir aux États-Unis.

Pendant que nous parlions de gouvernance du net et d'accès à la connaissance, cet objet à la fois diffus et précis que représentent les données a silencieusement transformé et refaçonné nos vies. Ces données, dans leurs multiples dimensions (personnelles ou ouvertes par exemple), sont d'abord apparues comme un nouvel or noir (« *data is the new oil* »), puis un nouveau terreau (« *data is the new soil* »), avant qu'on ne les qualifie de radioactives (« *data is the new uranium* »). Des acteurs sont en effet apparus, dont le modèle économique n'est autre que la prédation de données, notamment personnelles. Ils ont connu une croissance tellement gargantuesque qu'ils posent dorénavant un défi à la gouvernance au quotidien. Il nous semble primordial de garder en tête, quand on traite de souveraineté numérique, ce rapport de forces asymétrique, qui place en situation de vulnérabilité les individus mais aussi, de plus en plus, les administrations publiques et les entreprises.

Au vu de la complexité des enjeux interdépendants qu'elle implique, la question de la souveraineté numérique dépasse aujourd'hui le champ numérique traditionnel, des infrastructures et du web, pour toucher à la cybersécurité, à la neutralité du net, à la protection des données, à la lutte contre la désinformation, aux discours de haine, au multilatéralisme, à la fiscalité du numérique, aux technologies de rupture et à la transparence des algorithmes. Une telle conception de la souveraineté numérique correspond en tout cas à l'ambition que nous portons, à notre manière et à notre échelle, par la promotion d'une meilleure maîtrise du risque numérique, *via* la gestion des vulnérabilités.

La souveraineté numérique est partie intégrante de l'autonomie stratégique, qui dépasse quant à elle le modèle gaullien historiquement daté. Nous nourrissons une ambition claire : celle que la souveraineté française ne s'entende qu'en harmonie avec une souveraineté européenne. L'approche de la présidence française de l'Union européenne donne lieu à un alignement de planètes. J'en profiterai pour insister sur trois piliers constitutifs de la souveraineté numérique.

Le premier, politique, est aussi démocratique. Nos processus démocratiques apparaissent aujourd'hui des plus fragiles. Différentes mesures sont à l'étude pour protéger notre démocratie. Au-delà de cette approche conservatoire, il convient d'insuffler les valeurs démocratiques européennes aux initiatives technologiques et géopolitiques à venir. L'importance qu'attache Yes We Hack à la traçabilité des flux financiers relève de ce principe. Nous tenons au respect de la réglementation en matière de lutte contre le terrorisme et le blanchiment d'argent, en dépit de sa pesanteur souvent dénoncée. Elle traduit en effet nos valeurs, quitte à ce que d'aucuns voient parfois en elle un léger frein à la construction de notre offre de services. Nos valeurs d'éthique, de transparence et d'intégrité nous semblent un garde-fou nécessaire pour éviter que la construction d'un modèle européen ne tourne à la caricature d'une gestion d'entreprise à l'ancienne.

Le deuxième pilier de la souveraineté numérique, économique celui-là, touche à la prospérité commune. J'entends par là le fait de favoriser ou du moins de rendre possible une politique industrielle forte, qui capitalise sur la recherche scientifique. Le budget prévu par le fonds de relance européen complète dans cette optique d'autres instruments tels que le programme Horizon Europe ou DigitalEurope. La Commission présidée par Mme Ursula von der Leyen a fait du marché unique une priorité. Différentes initiatives plus ou moins avancées participent déjà à sa construction. En matière de cybersécurité, citons la démarche, soutenue

par le *Cyber Act*, de certification européenne, en vue d'harmoniser le niveau de cybersécurité exigé dans l'Union européenne.

Le troisième et dernier pilier de la souveraineté numérique, pour le coup technologique, n'implique pas une autarcie technique mais vise à réduire notre dépendance, voire notre servilité actuelle vis-à-vis d'acteurs extra-européens, notamment américains. Différentes approches existent, qu'elles passent par la législation ou par la commande publique, sur les insuffisances de laquelle, tant au niveau national qu'européen, il faudra d'ailleurs absolument se pencher. La tâche ne s'annonçant pas simple, je souhaite bien du courage à la personne qui tentera de relever le défi. Sans doute avez-vous déjà, dans cette mission d'information, abordé la commande publique française. De plus en plus d'initiatives européennes, certes discrètes, s'attaquent heureusement au problème, autrement dit, cherchent un moyen d'implémenter un marché unique du numérique européen.

Le modèle européen d'une souveraineté numérique fondée sur ces principes doit apporter la preuve de sa fonctionnalité et de sa capacité à s'exporter, seule à même de garantir sa place dans le monde. Yes We Hack l'a démontré par son exemple.

C'est dans ce cadre à la fois civil et militaire qu'en tant qu'acteur français et européen de la cybersécurité, nous inscrivons notre exigence de maîtrise et de gestion du risque numérique. Celle-ci se décline en un versant relatif aux données et aux infrastructures, auquel s'ajoute une composante stratégique de préservation et de maîtrise des fournisseurs. La question transversale de la gestion des vulnérabilités constitue notre cœur de métier. Son importance s'est encore accrue depuis les récents travaux de l'OCDE auxquels nous nous sommes activement associés, mais aussi grâce à d'autres initiatives telles que l'Appel de Paris, auquel nous avons également pris part, dont M. l'ambassadeur Henri Verdier vous a déjà parlé.

Un grand nombre d'initiatives s'attellent à la question de la cybersécurité de manière à la fois constructive, défensive et innovante, en questionnant ce qu'il est possible de mettre en œuvre pour dépasser une vision protectrice de ce concept, dans une volonté d'innovation, comme cela a d'ailleurs été fait pour les données, voici dix ans.

M. Philippe Latombe, rapporteur. Comment estimez-vous aujourd'hui le niveau de cybersécurité en France et en Europe ? Une culture de la cybersécurité s'est-elle selon vous suffisamment développée dans les entreprises, les collectivités territoriales et les États ?

Mme Rayna Stamboliyska. Je m'efforcerai de rester polie. Plaisanterie à part, on constate bel et bien un sursaut, même s'il est dommage qu'il survienne dans certains cas en réaction à un incident qui oblige à se demander comment reconstruire un système d'information, comment protéger des données d'utilisateurs ou de patients. La conscience, inégale, du rôle clé de la cybersécurité, apparaît largement plus développée dans certaines administrations ou pays que dans d'autres.

Ceci nous ramène à la notion de pouvoir ou plutôt de volonté. Un besoin évident se fait jour d'un État stratège, d'une ligne de conduite globale à suivre. Beaucoup se découragent quand ils comprennent que la sécurité d'une installation n'est jamais acquise une fois pour toutes, mais qu'il faut au contraire l'améliorer constamment. La nécessité de soutenir, consolider et nourrir cette amélioration continue implique la poursuite d'objectifs liés à une stratégie globale, qui s'appuie sur des outils dont on ne pourra disposer qu'en recourant à la commande publique, aujourd'hui insuffisante.

Je ne songe pas ici aux difficultés que pose un référencement à l'Union des groupements d'achats publics (UGAP), par exemple, mais aux exigences de sécurité bien trop faibles, voire inexistantes, imposées aux fournisseurs de services et d'outils numériques susceptibles d'être sollicités pour des commandes publiques. L'absence, en 2021, d'exigence d'un niveau minimal de sécurité ou d'un maintien aux conditions opérationnelles et de sécurité de ce qui est acheté dans le cadre de la commande publique a de quoi désagréablement surprendre.

Certes, des initiatives voient le jour, comme celle du sénateur M. Laurent Lafon. Le texte de sa proposition de création d'un CyberScore devrait parvenir sous peu à l'Assemblée nationale. L'ANSSI, en France, est forte de sa capacité à décerner des certifications et des qualifications. Nous ne comprenons toutefois pas pourquoi cette cohésion ne se renforce pas plus pour fournir aux administrations des outils performants, ergonomiques et surtout fiables. Je constate peu de discussions ou de travail concret effectif sur cette pierre d'achoppement, sans doute en raison d'une absence de stratégie globale.

Le gouvernement français s'est déjà doté d'un administrateur général des données. Pourquoi ne pas imaginer une harmonisation des exigences en matière de cybersécurité sous l'égide d'un fonctionnaire général de la sécurité des systèmes d'information (FSSI) ? Il fixerait à tous des objectifs clairs, et communiquerait une vision tout aussi claire de l'adoption, par tous, des instruments existants. La seule mention du référentiel général de sécurité (RGS) fait aujourd'hui grincer des dents. Ses préconisations sont pour l'heure appliquées de manière pour le moins inégale et parfois insuffisante, pour ne pas dire « au lance-pierres ».

M. Guillaume Vassault-Houlière. Le besoin se manifeste aujourd'hui d'une sécurité opérationnelle. Une grande diversité de cultures cyber coexistent dans le monde. Les Anglo-saxons n'optent pas pour la même approche que les Latins, sans parler de ceux qui pratiquent la politique de l'autruche. Les solutions de cybersécurité ont été pour l'heure empilées en couches successives. La loi du net oblige ses acteurs à rester en permanence opérationnels. Chaque jour en apporte la preuve. La crise sanitaire a incité à la rationalisation des coûts mais aussi à l'équipement en outils opérationnels.

Certains pays européens semblent mieux à même de gérer les risques, du fait de leur culture. Je songe aux pays nordiques ayant historiquement intégré le concept de développement agile. L'activité de notre plateforme enregistre d'ailleurs une forte croissance dans ces pays. D'autres nations semblent plus figées dans leur attitude et plus lentes à évoluer. En 2021, tout le monde a compris qu'il fallait démystifier la cybersécurité et prôner dans ce domaine une cohésion nécessaire, qui passera forcément par une multiplicité d'acteurs. Les relations entre secteurs public et privé jouent un rôle majeur en générant de l'innovation et en permettant de former du personnel qualifié. Il en résulte un cercle vertueux. Par ailleurs, certains pays accélèrent leur développement en matière de cybersécurité plus que d'autres, malgré leur retard initial. Tout dépend aussi des acteurs sur lesquels chaque pays peut s'appuyer sur son territoire.

Aujourd'hui, la géopolitique, loin de se limiter aux acteurs traditionnels du champ, implique plus que jamais les entreprises, qui en transposent les tendances. Plus il existe de sociétés innovantes, plus celles-ci jouent un rôle moteur d'innovation globale, en matière notamment d'utilisation des outils cyber à l'échelle mondiale. Nous pouvons aujourd'hui nous appuyer en Europe sur les pays nordiques et sur des acteurs compétents et passionnés.

La diversité des acteurs publics et privés impliqués dans le projet de campus cyber assurera sa force. Cette diversité a déjà démontré son efficacité dans d'autres pays. Certes, la prise de conscience en matière de cybersécurité s'accélère, pour autant, il ne faut pas emprisonner la commande publique dans des outils dépassés constituant un frein technologique pour les États tenus de se numériser rapidement. La tendance est aujourd'hui à l'ouverture croissante des systèmes d'information et des données dans un souci de transparence et de confiance. Il faut, pour y parvenir, des outils adaptés, des entreprises adéquates, une stratégie globale cohérente avec les valeurs européennes et une volonté de transformer un monde où le commerce se développe parfois en dépit du bon sens.

Chacun de nous est un client de ces grandes entreprises du numérique. En tant que tels, nous avons le pouvoir de les amener à fléchir, du moins celles qui n'appliquent pas les valeurs qui nous tiennent à cœur ou ne créent pas un cercle vertueux pour l'évolution de la société.

M. Philippe Latombe, rapporteur. Impliquez-vous que l'État et les collectivités territoriales se sont numérisés à toute vitesse sans intégrer d'entrée de jeu la cybersécurité, dont ils se sont occupés en ajoutant des couches successives à leurs projets ? Estimez-vous que, pire encore, ils n'en tiennent peut-être même pas compte dans leur vision à court et moyen terme ?

M. Guillaume Vassault-Houlière. Il faut bien comprendre qu'on ne trouvera jamais deux entités, qu'elles soient publiques ou privées, disposant exactement du même système d'information. Ces systèmes conçus par des personnes différentes, et à chaque fois transposés, ne sont pas partout maintenus selon les mêmes principes. Leurs composants, en particulier dans la commande publique, devraient inclure leur maintien aux conditions de sécurité. De plus en plus de pays dressent des catalogues pour faciliter la commande publique, en tenant compte de ces exigences.

Aujourd'hui, le plan de relance cyber, piloté notamment par l'ANSSI, place les collectivités territoriales dans une situation dont je ne doute pas, pour avoir discuté avec nombre d'entre elles, qu'elles la jugent inconfortable : elles doivent se plier à des normes édictées au niveau national, que les éditeurs de solutions numériques ne sont pas forcément tenus de respecter. Des acteurs, tels que des collectivités territoriales, ne disposant pas, parmi leurs équipes, d'experts en la matière, ni du temps voulu pour se pencher sur la question, sont sommés de se numériser rapidement.

En réalité, il manque une stratégie globale pour garantir une sécurité de bout en bout. À chacun son métier. L'union fait la force. Chacun doit assumer ses responsabilités. Il me paraît crucial de le souligner. La vulnérabilité des données a aujourd'hui un impact sociétal. L'actualité l'a montré. Chacun doit se penser comme un acteur du changement plutôt que comme un simple vendeur indifférent au devenir des solutions numériques qu'il commercialise. Des changements s'observent heureusement déjà en France, en Europe et dans le monde, ce que nous constatons dans certains pays d'Asie où nous sommes présents.

Les soucis qu'a connus Singapour voici quelques années ont amené cette cité-État à une prise de conscience. La simplicité d'utilisation de certaines applications gratuites, c'est-à-dire où le produit n'est autre que l'usager lui-même, n'implique pas qu'elles soient sécurisées. La notion de sécurité *by-design* a été transposée dans le RGPD. Les obligations qu'il comporte doivent s'appliquer à l'ensemble des acteurs du numérique pour garantir la sérénité de la totalité des usagers.

M. Philippe Latombe, rapporteur. Voyez-vous aujourd'hui des pays d'Europe dont la France devrait suivre l'exemple en termes de bonnes pratiques ? Existe-t-il en Europe un pays capable de jouer dans le domaine de la cybersécurité un rôle moteur ? Le campus cyber est en cours de construction, mais il ne concerne que la France, or la souveraineté numérique se bâtira, vous l'avez dit, à l'échelle européenne. Avez-vous eu vent d'initiatives européennes allant dans le même sens ?

M. Guillaume Vassault-Houlière. Nous disposons déjà de tous les outils que l'on pourrait souhaiter. Je ne pense pas seulement à l'ANSSI. La France peut s'appuyer sur son expérience de transposition au niveau national d'outils efficaces. Des certifications européennes existent déjà. Il ne reste plus qu'à entrer en action. La nouvelle version de la directive *NIS* va entraîner des changements. Il ne faut pas créer un entonnoir mais concilier l'agilité et la capacité de réagir vite avec le respect de plusieurs niveaux d'exigence, qui passera par du marketing européen. Il convient de miser sur la cohésion globale des éléments déjà disponibles, et de suivre une stratégie de souveraineté et de coordination dépassant même le cadre strictement européen.

Mme Rayna Stamboliyska. Beaucoup de pratiques résultent de l'histoire et de la culture propres à chaque pays. Prenons le cas de l'Allemagne, notre plus proche allié européen, avec qui nous partageons une frontière. Sa structure fédérale en Länder implique une organisation des administrations tout à fait différente de ce qu'on observe en France. Dans chaque pays coexistent des usages dont il y a lieu de s'inspirer et d'autres, plus critiquables. Il m'apparaît nécessaire de mener une réflexion collégiale au côté de nos homologues européens pour éviter de rédiger des feuilles de route nationales qui perdront de leur pertinence lorsqu'une mise en conformité aux normes européennes s'imposera.

L'exemple de la fiscalité du numérique le montre assez. Les transpositions nationales divergentes de la directive *NIS* avaient donné lieu à des incohérences problématiques. Plusieurs ateliers se sont attelés l'an dernier à sa révision et à la reformulation de ses exigences. Nous nous y sommes d'ailleurs impliqués. Certains opérateurs de services essentiels en France ignoraient si leurs homologues aussi étaient considérés comme tels dans d'autres pays. Les agences de cybersécurité (les ANSSI locales) édictaient dans chaque pays leurs propres exigences. Des Polonais ont ainsi réclamé aux Français des preuves de conformité au sein d'un même groupe. D'aussi considérables variations, d'une législation nationale à l'autre, apparaissent ingérables et mènent à la catastrophe. On comprend dès lors mieux pourquoi, au moment de réviser la directive *NIS*, d'aucuns ont argumenté en faveur de sa transformation en Règlement, de manière à l'appliquer sans presque aucune modification d'un pays à l'autre. Le texte parvenu au Parlement reste pour l'heure une directive. Toutefois, son périmètre élargi l'amène à concerner de plus nombreux secteurs, ce qui contribue à une meilleure harmonisation des pratiques.

C'est à de tels niveaux qu'il faut transmettre au reste de l'Europe ce que l'expérience de la France lui a appris. La loi de programmation militaire (LPM) a, dans sa version 2014-2019, défini de manière inédite les systèmes d'information d'importance vitale. Autrement dit, une composante technique et cyber est entrée pour la première fois dans cette loi de financement. Cette LPM a impulsé la première mouture de la directive *NIS*. La révision de cette dernière, en discussion, prend appui sur les leçons positives et sur d'autres, tirées des dysfonctionnements liés à la notion de *lex specialis,* selon laquelle prévaut la loi spécifique à un domaine, en l'occurrence nationale.

Lors des ateliers de révision de la directive *NIS*, j'ai avancé comme exemple concret l'appel d'air créé pour les entreprises par la LPM en France. Les exigences inscrites dans cette loi se sont ajoutées à d'autres édictées par l'ANSSI en matière de sécurité des fournisseurs, de services de sécurité ou d'équipement, aux opérateurs d'importance vitale. Des opportunités de développement commercial non anticipées en ont résulté.

On croit en général que l'application d'exigences réglementaires entraîne des frais et prend du temps. On en oublie de considérer leur impact dans son ensemble. Les fournisseurs contraints d'élever leur niveau de sécurité obtiennent au final un retour sur investissement, dans la mesure où ils captent ainsi de nouveaux clients. Il faut en tenir compte dans les discussions en cours sur la construction technologique européenne. On peut s'inspirer, dans le même ordre d'idées, de l'exemple néerlandais en matière de divulgation des vulnérabilités, ou des pratiques allemandes en ce qui concerne la commande publique fédérale.

M. Philippe Latombe, rapporteur. L'État a fait appel à vous pour la mise au point de l'application StopCovid. Faut-il y voir une initiative ponctuelle ou le signe d'un changement de paradigme ? L'État adopte-t-il enfin progressivement une méthode plus agile ? Le recours à vos services vous semble-t-il appelé à perdurer ou à s'intégrer dans le champ de réflexion de l'administration ?

M. Guillaume Vassault-Houlière. Notre rôle dans le lancement de l'application TousAntiCovid, particulièrement médiatisé du fait de l'exigence de transparence et de confiance qu'imposait la généralisation de cet outil, à l'origine, dans un premier temps, d'une certaine défiance, ne constitue qu'un exemple parmi d'autres.

En ce qui concerne l'application StopCovid, les autorités nous ont donné carte blanche pour transposer notre expertise et tout s'est très bien passé. Nous avons noué d'excellentes relations avec les équipes de l'ANSSI et de l'Institut national de recherche en informatique et en automatique (Inria), qui nous ont au final accordé leur confiance, après de nombreux débats sur la question complexe des tests auxquels nous souhaitions soumettre l'application. Ceci dit, cette collaboration ne nous a pas fourni l'opportunité de démontrer l'étendue de notre savoir-faire.

Suite à un incident de sécurité survenu avec la messagerie Tchap, nous avons soumis cet outil public à la communauté des 22 000 *hackers* de Yes We Hack afin de trouver une parade à ses vulnérabilités, de manière à rassurer ses utilisateurs. Nous avons également noué un partenariat avec l'état-major des armées (EMA), c'est-à-dire le commandement de la cyberdéfense. Mme la ministre a d'ailleurs divulgué, en 2019, son recours à des *hackers* éthiques, *via* notre plateforme, en vue de sécuriser différents périmètres du ministère. D'autres administrations encore font appel à notre communauté, forte de son opérationnalité.

En tant que pur produit de la communauté des *hackers* des années 2000, passionné par mon métier, je me rends bien compte, pour avoir travaillé avec des entités ministérielles de France et d'ailleurs, que nos concitoyens éprouvent le besoin d'outils fiables au fonctionnement transparent. Nous nous devons aussi de sécuriser les données, au volume sans cesse croissant. La France a joué un rôle précurseur à travers le commandant de la cyberdéfense, lorsqu'il a cherché comment animer et former les 400 réservistes à sa disposition, et comment élargir les tests de sécurité de ses outils numériques, jusque-là réalisés en interne *via* des audits planifiés. La perception du risque progresse à la vitesse à laquelle se développent les nouvelles technologies. Un besoin se fait jour de compétences adaptées rattachées à des métiers divers et variés.

Le stéréotype du méchant *hacker* ne prédomine plus du tout aujourd'hui comme c'était le cas dix ans plus tôt. Notre communauté incarne une philosophie et un art de vivre dépassant le simple cadre de l'informatique et impliquant la remise en cause perpétuelle de notre écosystème dans la volonté de l'améliorer.

L'article 47 de la loi pour une République numérique protège les lanceurs d'alerte s'adressant à l'ANSSI. Jusque-là, certains *hackers* ne voulaient plus courir le risque de signaler des vulnérabilités aux entreprises ou aux entités ministérielles par crainte de poursuites pénales. Leur action citoyenne n'était en effet pas comprise. Aujourd'hui, de plus en plus de pays cherchent un moyen de dénoncer les vulnérabilités *via* la création de canaux de communication de confiance avec les communautés de *hackers*.

Nous avons réussi avec d'autres experts mondiaux à transposer de telles initiatives dans une note d'un rapport de l'OCDE. L'*European Union Agency for Cybersecurity (ENISA)* se penche en ce moment même sur des changements à venir. La France a joué un rôle moteur précurseur avec les Néerlandais. L'accroissement des menaces pousse à se tourner vers des outils de plus en plus efficaces garantissant un retour sur investissement rapide. La plateforme Yes We Hack, parfaitement adaptée au monde actuel, a déjà prouvé son efficacité.

Tout le monde souhaite embaucher les meilleurs spécialistes de la cybersécurité. Je rappelle que quatre millions de postes demeurent à ce jour à pourvoir dans ce domaine, sur l'ensemble de la planète. La numérisation croissante de la société et des États génère un fort besoin de cybersécurité. Nous travaillons en ce moment sur des dispositifs de vote en ligne. Il n'est plus envisageable de s'en remettre à l'expertise d'une seule entreprise. Il convient au contraire de solliciter une communauté de passionnés, dans toute sa diversité. Nous savons tous que l'union fait la force. L'intelligence collective a démontré son efficacité dans beaucoup de domaines. Nous sommes très fiers que les acteurs étatiques aient compris notre démarche et fassent appel à nos services.

Œuvrer en partenariat avec le ministère des armées relevait d'un rêve d'enfant. Aux États-Unis, de nombreux *hackers* souhaitaient s'attaquer au Pentagone. Des initiatives américaines relatives à l'*US Air Force* ont vu le jour. Nous avons quant à nous réussi à mettre en avant, auprès du ministère des armées, notre modèle fondé sur des valeurs françaises et européennes et sur la confiance, pour œuvrer en bonne intelligence avec la communauté de l'EMA.

Nous préconisons que tout outil commercialisé au grand public, y compris les voitures, dispose d'un outil de signalement de ses vulnérabilités afin d'éviter toute utilisation malveillante. Nous prônons aussi de placer à l'abri des poursuites judiciaires tout citoyen révélant une faille de sécurité. On assiste en somme à un changement sociétal. Chaque État avance désormais, certes à sa vitesse, dans la bonne direction. La remarque est transposable aux ministères et à d'autres strates administratives encore. Nous nous efforçons depuis des années de montrer ce que peut apporter une collaboration avec des *hackers* de bonne volonté.

M. Philippe Latombe, rapporteur. Nous avons auditionné la semaine dernière l'Imprimerie nationale et, quelques jours auparavant, la responsable du projet « identité numérique ». Cette identité numérique vous apparaît-elle comme une opportunité ou plutôt comme une faille ? Comment percevez-vous ce projet en termes de cybersécurité ? Constitue-t-il un point de vigilance supplémentaire ? Les pays qui l'ont adoptée s'y sont-ils pris de manière suffisamment sécurisée ?

J’ai jusqu’ici recueilli deux réponses fort éloignées à mes questions. La responsable interministérielle affirme que la mise en place de l’identité numérique passera par des marchés exclusivement publics, alors que l’Imprimerie nationale avance que les entreprises privées y auront leur place. Les données liées à l’identité numérique, du fait de leur considérable importance, ne feront-elles pas l’objet d’attaques permanentes mobilisant des technologies de plus en plus avancées ? Que vous inspire sa mise en place, en France et dans d’autres pays, en Europe et ailleurs ?

M. Guillaume Vassault-Houlière. Il faut aujourd’hui, pour minimiser le risque, immuniser les données. Il convient de déterminer, dans chaque projet, les mesures de sécurité qui relèvent ou non de l’utile. L’identité numérique sera attaquée au même titre que tout vecteur, peut-être plus encore en raison de la quantité de données qui y sont liées. L’identité numérique implique une interconnexion avec différents satellites, IdP (*identity provider*) et SP (*service provider*). Il faudra donc sécuriser toute la chaîne. En réalité, le risque zéro n’existe pas.

Je prône dans tous les cas d’atteindre l’efficacité par les moyens les plus simples. Je m’interroge à ce titre sur l’intérêt d’imposer des mesures de sécurité additionnelles uniquement pour ne pas confier la gestion de l’identité numérique à un seul et unique acteur global.

J’ai travaillé dans la haute disponibilité durant de nombreuses années. Mes clients exigeaient de moi, il y a quinze ans, de la réversibilité et de la résilience, la seconde supposant de toute façon la première. Peu importe le nombre d’acteurs impliqués dans un projet, à partir du moment où son niveau de documentation et d’interopérabilité atteint un certain seuil, le risque apparaît maîtrisé. Chacun a les mêmes exigences techniques, en matière de cybersécurité comme de stockage. Il me semble important de construire un projet qui en tienne compte. On en revient à la souveraineté. Il faut bien analyser et gérer le risque dès le début du projet, ce que résume d’ailleurs parfaitement le concept de sécurité *by-design*, et garantir la réversibilité en cas de problème.

L’identité numérique relève désormais d’une nécessité. Il convient toutefois de l’utiliser avec parcimonie, dans un premier temps, de manière à capitaliser sur les projets à venir pour garantir son efficacité, plutôt que de laisser l’initiative à des acteurs incompétents, incapables de garantir ne serait-ce que nos numéros de téléphone. Les identités numériques qu’ils gèrent sont censées permettre l’accès à une multiplicité de service ; or ce sont toujours les mêmes qui gardent la mainmise dessus. Nous avons la chance de disposer de l’excellente initiative Franceconnect. Il faut continuer en ce sens. Il m’apparaît tout à fait possible d’aboutir à une réalisation susceptible de servir de modèle, en Europe comme dans le reste du monde, en s’appuyant justement sur les valeurs européennes.

Mme Rayna Stamboliyska. Je ne suis pas du tout spécialiste de l’identité numérique. Je m’excuse donc par avance des inexactitudes qui m’échapperaient.

Il m’apparaît nécessaire de clarifier rapidement le modèle économique sur lequel repose l’identité numérique. La révision du Règlement sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) le montre assez. Elle pourrait d’ailleurs figurer parmi les actions notables portées par la future présidence française de l’Union européenne.

On évalue le marché de l'identité numérique à un peu plus d'un milliard d'euros de revenus à l'horizon 2030. Une question se pose : comment permettre aux acteurs français et à l'État de mettre en œuvre une structure économique susceptible de préserver ce marché face à des initiatives déjà lancées par des acteurs privés extra européens tels que Google, Apple, Facebook, Amazon et Microsoft (les GAFAM) ?

Le scénario le plus probable m'apparaît encore être celui où le schéma de l'identité numérique se structurerait autour d'un fédérateur d'identité unique offrant aux utilisateurs le choix d'un fournisseur d'identité, dans l'hypothèse d'un Règlement eIDAS substantiel aux exigences élevées. Ce fournisseur, public ou privé, permettrait d'accéder à l'ensemble des services publics et privés.

Une autre question émerge dès lors : celle des garanties dont bénéficieront les données des citoyens français et européens. Là encore, l'ANSSI tient lieu de source d'inspiration avec sa récente publication d'un référentiel d'exigences en matière de sécurité de l'identité numérique. Dans la révision du Règlement eIDAS, il apparaît primordial de continuer à promouvoir un niveau élevé de sécurité et de préserver les fournisseurs d'identité privés au sein de l'Union européenne, à condition bien sûr qu'ils soient réellement européens et non de simples entités juridiques au siège sis en Irlande ou au Luxembourg. L'identité numérique fonctionne à une double échelle, nationale et européenne.

Franceconnect peut assumer en France un rôle important, aussi bien d'acteur assurant l'ensemble des fonctions requises, que de *hub* technique pour les fournisseurs.

Quoi qu'il en soit, il est impératif de maintenir au niveau européen les exigences du Règlement eIDAS, destiné, en l'état, à prévenir l'apparition de fournisseurs d'identité numérique extra européens privés. À cela doit s'ajouter ce qui émerge à travers la stratégie européenne relative aux données, les préconisations de l'ANSSI en France, ainsi qu'un projet du ministère de la transformation et de la fonction publique, à savoir l'idée d'un *cloud* au cœur de l'État, imposant clairement une exigence de localisation de données sur le territoire européen, voire dans le pays concerné. Ce projet obéit au mot d'ordre du commissaire, M. Thierry Breton, soucieux que les données des pays européens restent en Europe.

Il faudra, pour y parvenir, livrer une grande bataille, qui s'avère d'autant plus indispensable qu'aujourd'hui, 90 % des données produites en Europe, personnelles ou non, ne sont pas stockées sur le continent européen, encore moins par des acteurs européens. Il faut s'assurer que la révision du Règlement eIDAS et de la directive *NIS*, la stratégie européenne en matière de données et les initiatives entre autres françaises dans ce domaine demeurent en cohésion et en harmonie pour se soutenir mutuellement, afin d'éviter la dispersion des capacités, de manière à permettre l'émergence d'un modèle économique hybride acceptable par une majorité d'acteurs européens et par les citoyens eux-mêmes.

On a pu constater une défiance de certains vis-à-vis du rôle de l'État en tant que responsable du traitement des données, contrastant avec leur méfiance moindre envers certains acteurs privés d'envergure. À l'inverse, l'État inspire à d'autres moins de doutes que certaines entreprises privées.

Il semblerait donc intéressant de construire un modèle hybride associant, à la fonction étatique publique, la fourniture de services, en l'occurrence d'identité numérique, par des acteurs privés, en conformité avec des exigences réglementaires et législatives européennes communes, impulsées par les États.

M. Philippe Latombe, rapporteur. Il faut aussi se demander si l'identité numérique fera l'objet d'attaques, quoique M. Vassault-Houlière ait déjà répondu à cette question par l'affirmative, en raison du profit qui pourrait être retiré de son usurpation.

Les attaques d'hôpitaux et de collectivités territoriales se sont multipliées dernièrement, sans même parler de l'incendie d'OVH. Il est apparu que beaucoup d'entreprises et d'administrations ne disposaient ni de plan de reprise d'activité (PRA) ni de plan de continuité d'activité (PCA). Il a beaucoup été question des attaques russes contre le centre national d'enseignement à distance (CNED) et des problèmes de connexion aux espaces numérique de travail avant-hier.

Les mesures de sécurité mises en place aujourd'hui vous semblent-elles suffisantes ? N'avez-vous pas le sentiment d'une perte de certains réflexes ? Du temps où l'on ne disposait que d'archives papier, il était d'usage d'en réaliser des copies. La généralisation du numérique ne nous a-t-elle pas rendus naïfs ou imprévoyants à certains égards ? Ne faudrait-il pas, selon vous, réintroduire dans nos habitudes quelques règles de bon sens ?

M. Guillaume Vassault-Houlière. Je vous répondrai par l'affirmative. Ceci dit, votre remarque ne s'applique-t-elle pas aussi aux téléphones ? Beaucoup, par méconnaissance ou pour gagner du temps, installent sur leurs appareils des applications qu'ils ne maîtrisent pas. Il me paraît important de démystifier les questions de sécurité. Nous devons creuser sous la surface, loin de nous fier aux apparences.

L'anticipation de menaces ou de soucis techniques n'est jamais simple.

L'incendie d'OVH a impacté notre activité. Nous étions toutefois préparés à une telle éventualité, vu que la construction d'infrastructures indestructibles relève des préoccupations de notre métier. J'ai la chance de disposer d'équipes techniques performantes, qui ont résolu rapidement les problèmes.

Les achats, aujourd'hui facilités, ne s'effectuent plus dans les mêmes conditions qu'avant. Le métier de la haute disponibilité souffre d'une méconnaissance. Pour l'anecdote, j'ai mis en place des infrastructures destinées à la presse et aux citoyens, en vue de l'annonce des résultats d'élections, voici dix ans. La haute disponibilité n'est pas un sujet simple à aborder, surtout si l'on y inclut les risques d'attaques. Je ne jette la pierre à personne. Les PRA et PCA ont un coût. La question des compétences dans le numérique ne concerne pas que la cybersécurité mais aussi les infrastructures.

Indépendamment du recours au *cloud*, il existe de bonnes pratiques, entre autres d'achat. Il convient de se poser les bonnes questions. Selon moi, il appartient aux établissements de formation de revenir aux bases. Quand on construit une infrastructure, il faut penser à sa résilience, à l'analyse des risques, ce que l'on faisait à l'époque où l'on avait affaire à des serveurs physiques. La virtualisation liée à l'usage du *cloud* rend ces risques moins palpables, or en tant qu'êtres humains, nous éprouvons le besoin de toucher du doigt les menaces pour nous les représenter. Au final, on ignore où sont stockées les sauvegardes, ni même si elles existent. Ces questions relèvent d'une problématique de transparence. Tout est lié. La situation ne s'améliorera pas d'elle-même. Il nous appartient à nous, acheteurs, de poser les bonnes questions.

Il a beaucoup été question de réversibilité à propos du RGPD, toutefois, ce concept s'est quelque peu égaré dans les méandres de l'histoire des infrastructures. Nous devons nous

demander où sont stockées nos données. Il nous revient à nous, acheteurs, de changer les habitudes liées à l'usage des plateformes *software as a service* (SaaS). La transparence engendrera la confiance. Ensemble, elles constituent les meilleures alliées du marketing.

Il n'en faut pas moins garder à l'esprit que toute une catégorie d'acteurs comme les collectivités territoriales, dont la cybersécurité n'est pas le cœur de métier, n'ont pas les moyens de se pencher sur ces questions, ce qui les oblige à s'en remettre à leurs fournisseurs. Ces acteurs accordent leur confiance aux experts qu'ils ont mandatés. Il faudrait peut-être revenir aux *requests for proposal* (RFP), c'est-à-dire aux appels d'offres tels qu'ils étaient rédigés voici quinze ans. Leurs exigences d'alors sont depuis passées à la trappe, car il est plus facile de passer une commande en quelques clics. Il ne faut toutefois jamais perdre de vue les principes fondamentaux de construction d'une architecture, tels que la disponibilité ou la résilience.

M. Philippe Latombe, rapporteur. Voyez-vous des sujets que nous n'aurions pas abordés, que vous souhaiteriez mettre en lumière ?

Mme Rayna Stamboliyska. Il nous apparaît vraiment urgent et nécessaire de disposer d'une feuille de route concrète, aussi bien au niveau national qu'européen.

Quand on commence à regarder de plus près ce qui se passe au niveau européen, comme m'y oblige par chance mon travail, on voit comment les différentes entités et structures s'imbriquent et s'interfacent. Cependant, nous ne sommes qu'un petit nombre à disposer d'une telle vision. Il m'apparaît donc impératif d'édicter une feuille de route claire, dans l'esprit de l'annonce, par le président Emmanuel Macron, du milliard d'euros consacrés à un plan global en matière de cybersécurité. Il manque aussi davantage de communication simple et accessible, à destination des administrations, des entreprises du CAC 40, des collectivités territoriales, des hôpitaux et des usagers, etc.

Nous continuerons à voir des hôpitaux victimes d'attaques nous concernant tous, dans la mesure où nous sommes tous des patients, tant que nous ne prendrons pas conscience que les outils numériques incluent aussi l'ordinateur de la secrétaire ou le téléphone du directeur, puisqu'eux aussi permettent à l'infrastructure de fonctionner. Au-delà des serveurs ou des câbles, de tels composants structurels ne sauraient pâtir plus longtemps de notre négligence, tout cela parce qu'il nous manque le temps, l'envie ou l'argent pour nous en préoccuper.

Il nous faut en somme une feuille de route concrète, indiquant des objectifs précis et les moyens de les atteindre, et détaillant les actions opérationnelles à réaliser par différents acteurs, de même que leurs sources de financement. Une telle feuille de route devrait faire la part belle à la recherche et à l'innovation. Nous parlons de souveraineté numérique à l'échelle européenne, or l'avenir se construit dès aujourd'hui et, pour y parvenir, il faut réfléchir à la dette technique, technologique et décisionnelle qui nous poursuit depuis des années, mais aussi à notre manière de préparer et de concevoir le futur proche.

Il est beaucoup question aujourd'hui de 5G. Je n'évoquerai pas les théories complotistes selon lesquelles il faudrait se faire vacciner pour en disposer. Heureusement, la réalité leur oppose un démenti. Une dette technique nous handicape, qu'il faut éponger vite et bien sans en générer de nouvelle.

L'indispensable feuille de route nationale et européenne que nous appelons de nos vœux doit aussi prévoir selon quelles modalités, à l'avenir, s'opéreront les justifications

d'identité, les connexions, l'envoi de données, la maîtrise des interconnexions entre différentes entités, en somme, comment le risque cyber sera géré. On parle souvent de boîte à outils 5G. Que signifie concrètement ce terme ? Comment le fonds de relance européen se décline-t-il au niveau national ? Comment développer le volet technologique de manière à ce qu'on puisse se saisir des leviers aujourd'hui disponibles, souvent réglementaires et en tout cas légaux, afin d'aboutir à une réalisation concrète que tout le monde soit en mesure d'utiliser ?

M. Guillaume Vassault-Houlière. Les enjeux du numérique, dont la cybersécurité, concernent tous les pans de la société. Nous disposons de tous les leviers et de tous les acteurs voulus, sans même parler de l'intelligence collective, pour avancer dans la bonne direction. Il ne reste plus qu'à donner un coup d'accélération au processus.

Il faut continuer, surtout, à prôner la cohésion. Ensemble, nous sommes plus forts. La remarque vaut pour l'Europe, mais pas seulement. La transparence revêt une importance cruciale. Il faut faire confiance à la communauté de passionnés de cybersécurité que nous défendons depuis des années et dont je fais moi-même partie.

Je salue tous ceux qui mettent du cœur à l'ouvrage pour sécuriser les différentes infrastructures en gardant leur esprit critique constructif. Il faut continuer à démystifier la profession de *hacker* pour que tout le monde comprenne que ce merveilleux métier conviendra à tous ceux qui ont soif d'apprendre au quotidien, à base d'échanges, car il ne s'agit pas d'œuvrer seul dans son coin.

Notre communauté a montré sa capacité à innover et à améliorer le quotidien de tous depuis des années. La communauté des radioamateurs partageait la même philosophie. Nous lui devons aujourd'hui des quantités de brevets. Nous souhaitons tous aboutir à des réalisations intelligentes. Passons à présent à des actions concrètes en assurant, encore et toujours, la promotion de nos valeurs européennes partout dans le monde. Des acteurs d'autres pays parviennent très bien à diffuser leur culture.

Notre petite entreprise, qui a connu une croissance fulgurante, évolue dans un monde où règne une exigence de confiance et de transparence majeure. Élargissons aujourd'hui nos initiatives au plus haut niveau et prouvons notre capacité à construire un système opérationnel dans un monde en accélération constante. Protégeons enfin ces passionnés de cybersécurité pour qu'ils continuent de garantir la transparence de tous les outils numériques mis à notre disposition, afin de protéger à leur tour notre quotidien, aujourd'hui comme à l'avenir.

La séance est levée à 12 heures 40.

Membres présents ou excusés

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

Réunion du jeudi 8 avril à onze heures

Présents. – M. Philippe Latombe

Excusée. – Mme Frédérique Dumas