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 9 heures 30

Compte rendu n° 55

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA)

La séance est ouverte à 9 heures 30.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. M. Jérôme Notin, la structure dont vous êtes le directeur général, plus connue sous le nom de cybermalveillance.gouv.fr, correspond au dispositif national d'assistance aux victimes de cybermalveillance, et de sensibilisation des publics au risque numérique. Dans nos travaux sur les enjeux de cybersécurité, votre audition s'inscrit à la suite de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la fédération française de la cybersécurité.

Nous souhaitons échanger avec vous sur l'état de la menace cyber, les modalités d'accompagnement des victimes, déployées par votre dispositif, et la nécessité de promouvoir une véritable culture de l'hygiène numérique auprès des acteurs publics et privés.

M. Philippe Latombe, rapporteur. Je commencerai par vous poser une question rituelle : comment définiriez-vous la souveraineté numérique ? J'aimerais que vous nous présentiez ensuite le groupement Action contre la Cybermalveillance (ACYMA), son actualité et son fonctionnement. Comment soutenez-vous les victimes de cyberattaques ? Comment collaborez-vous avec les acteurs publics également chargés de la question en France, mais aussi en Europe ? Des pratiques de coopération ou d'échanges ont-elles cours avec vos homologues dans d'autres États membres de l'Union européenne ?

Je souhaiterais en outre établir un bilan de la menace en revenant sur les principaux types d'attaques répertoriés, leurs évolutions durant la crise sanitaire et le profil des victimes qui se tournent vers vous.

J'aimerais dans un second temps que nous prenions du champ par rapport à la cybersécurité. Le gouvernement vient d'annoncer qu'il lui consacrera des moyens renforcés dans sa stratégie nationale cyber. Comment percevez-vous cette initiative ? J'aimerais que vous évoquiez votre tout nouveau label ExpertCyber, attestant l'expertise numérique de prestataires cyber.

Enfin, je voudrais aborder la diffusion d'une culture cyber au sein de la société. Quel regard portez-vous sur le degré de sensibilisation à la cybersécurité, aussi bien des entreprises et des administrations publiques, dont les collectivités territoriales, que des citoyens ?

Je voudrais pour conclure évoquer la formation en compétences cyber, puisqu'un campus cyber devrait bientôt voir le jour avec l'appui, entre autres, de l'ANSSI. Comment se positionne la France sur ces enjeux par rapport à d'autres pays ? Devrions-nous compléter notre offre de formation dans certains segments en particulier ou combler des lacunes que vous auriez identifiées ?

M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA). La souveraineté implique selon moi de disposer de produits inspirant à juste titre la confiance. La création de votre mission prouve en soi qu'il reste de véritables besoins à couvrir dans ce domaine. On trouve bien quelques acteurs français et européens de cybersécurité, mais il subsiste de nombreux « trous dans la

raquette ». Ni les particuliers, ni les entreprises, ni les collectivités territoriales ne disposent pour l'heure d'une offre à cent pour cent souveraine. Un travail considérable reste à mener.

La France a la chance de disposer de compétences entrepreneuriales et d'expertise technique en cybersécurité, mais qui ne se rencontrent pas forcément. Je ne peux qu'engager à poursuivre vos travaux pour que, dans les années à venir, la France jouisse enfin d'une souveraineté nationale en ce domaine.

Notre groupement d'intérêt public s'est donné pour objectif de faire savoir à nos concitoyens (collectivités territoriales, entreprises ou particuliers) qu'en cas de problème de cybersécurité, notre plateforme « .gouv.fr » est en mesure de les aider.

Trois missions nous ont été confiées suite à la présentation de la stratégie nationale pour la sécurité du numérique en 2015 :

– L'assistance aux victimes passe essentiellement par la plateforme cybermalveillance.gouv.fr. Toute victime qui s'y connecte suit un parcours défini : elle renseigne son profil, puis répond à quatre ou cinq questions permettant d'établir un diagnostic, après quoi, soit nous lui fournissons des conseils, si elle est en mesure de les appliquer de manière autonome, soit nous la dirigeons vers internet-signalement.gouv.fr ou la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), puisque nous avons vocation à constituer un fichier unique. Surtout, quand une assistance technique s'avère nécessaire, nous proposons une mise en relation avec des prestataires de proximité. Notre plateforme en référence aujourd'hui un millier, en mesure d'aider aussi bien des particuliers que des entreprises ou des collectivités territoriales, victimes de l'une des 45 formes de cybermalveillance répertoriées. Nous avons réussi à glisser dans le dossier de presse complétant les annonces du président de la République la création du label ExpertCyber, dont bénéficient aujourd'hui 55 prestataires aux compétences vérifiées.

– Dès la création de notre dispositif en 2017, nous avons produit beaucoup de contenus de sensibilisation, sous licence ouverte, dès que leur format le permettait. Une partie de nos publics, notamment les collectivités territoriales, nécessite encore de prendre conscience du risque cyber. Certains élus se croient à l'abri d'une attaque, du fait qu'ils ne détiennent pas de propriété intellectuelle ou de fichier clients, donc de données susceptibles *a priori* d'intéresser des pirates. Ils se trompent. Pendant le premier confinement, en avril et mai 2020, nous avons, grâce à France Télévisions, à TF1 et au groupe Canal+, diffusé de brefs messages de sensibilisation.

– Notre troisième mission est la mise en place d'un observatoire de la menace, afin d'analyser celle-ci aussi exhaustivement que possible, et va s'accélérer en 2021. Le ministère de la justice a d'ores et déjà mis à notre disposition un agent dans cette optique. Personne ne sait aujourd'hui qui visent les attaques, ni ce qu'elles coûtent à l'économie française, à l'État ou à l'Europe.

M. Philippe Latombe, rapporteur. Que les confinements nous ont-ils appris en matière de sensibilisation ? Avez-vous noté une amélioration de la prise de conscience au fil du temps ? Les entreprises, et je pense plus à celles de petite taille qu'aux grands groupes sans doute mieux avertis, utilisent-elles plus volontiers des réseaux privés virtuels (VPN) ? Ont-elles compris qu'il ne fallait pas se servir d'un ordinateur personnel à des fins professionnelles ?

Les collectivités territoriales qui lancent en ce moment même de nombreux projets de villes intelligentes (ou *smart cities*) y intègrent-elles la cybersécurité dès le départ ? Ou n'y songent-elles qu'à la fin, après avoir pris conscience qu'elles ont oublié de se doter d'une « porte blindée » ?

Que s'est-il passé mardi dernier sur les espaces numériques de travail et les plateformes d'école à la maison ? Il était peut-être maladroit de rejeter la faute de l'incident sur OVH. Les attaques russes contre le centre national d'enseignement à distance (CNED) semblent brandies comme excuse, peut-être en partie à juste titre. N'y recourt-on pas toutefois par facilité, pour masquer les défaillances de l'architecture du site ?

M. Jérôme Notin. Je garderai pour moi ce que m'inspire cet incident et me contenterai de rappeler les faits : une recrudescence de connexions légitimes à la plateforme du CNED et à ses sites satellites a fait peser sur les serveurs une forte charge. Le ministre a évoqué des cyberattaques de l'étranger. La chaîne sécurité des systèmes d'information (SSI) du ministère m'a confirmé la réalité d'une attaque par déni de service (DDoS). Le ministère a déposé plainte auprès du parquet chargé de la cybercriminalité.

Je me permettrai une digression : s'il existe en France un axe d'amélioration de la cybersécurité, et donc, de la souveraineté qui en découle, il réside auprès du parquet. Par chance, celui-ci a pris conscience de la nécessité de disposer de magistrats spécialisés. D'une remarquable compétence, ils accomplissent un travail extraordinaire. Malheureusement, ils ne sont que trois. Il en faudrait bien plus.

M. Philippe Latombe, rapporteur. Combien selon vous ?

M. Jérôme Notin. La question s'adresse peut-être plus aux magistrats eux-mêmes. J'estime qu'une dizaine d'entre eux auraient encore fort à faire pour que la justice se saisisse des affaires comme il se doit, identifie les auteurs des infractions et y mette un terme. Un parquet renforcé serait en mesure de traiter aussi bien la petite cybercriminalité (les arnaques visant les particuliers) que les attaques étatiques contre les infrastructures régaliennes de la France, sans oublier celles dont le CNED a fait les frais.

M. Philippe Latombe, rapporteur. Ces magistrats disposent-ils d'outils judiciaires adaptés ? Au-delà de la question des effectifs, sont-ils capables de réagir rapidement ou, à l'inverse, de s'accorder du temps quand une investigation le requiert, et de mobiliser les experts indispensables aux enquêtes ?

M. Jérôme Notin. Je les crois en mesure, par le biais de l'ANSSI, de saisir les experts les mieux à même de les seconder. Ils disposent en outre du meilleur policier de France en matière de rançongiciel, en sa qualité d'assistant technique du parquet.

En revanche, les outils juridiques pourraient être améliorés. Nous cherchons à créer un groupe de travail réunissant des représentants des ministères de la Justice et de l'Intérieur, des opérateurs, des associations de victimes et des fédérations professionnelles, pour traiter de l'hameçonnage. Nous estimons les tentatives d'hameçonnage insuffisamment prises en compte, sans doute faute d'un outil législatif adapté, alors que cette forme de cyberdélinquance sert de point de départ à nombre d'autres attaques.

De faux sites de vente de gel et de masques ont proliféré en pleine pénurie, pendant le premier confinement. On connaît l'extraordinaire capacité d'adaptation des cybercriminels.

Dès le soir du 16 mars, notre plateforme a constaté une multiplication par cinq des tentatives d'hameçonnage, dénoncées par des victimes cherchant auprès de nous de l'aide. Nous avons formé à leur répression la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), qui ne pouvait hélas que couper l'accès à ces plateformes frauduleuses. Dix nouvelles autres les remplaçaient aussitôt. La justice ne s'est pas saisie de ces affaires, faute d'un outil législatif permettant d'identifier les coupables. La loi a évolué depuis. Mais cette absence d'une législation adaptée pose un réel problème aux collectivités territoriales et aux entreprises victimes de tentatives de récupération des mots de passe en vue d'installer un rançongiciel qui bloquera leur activité. Empêcher les cybercriminels de récupérer des données, personnelles, professionnelles ou institutionnelles marquerait un formidable bond en avant, en limitant considérablement leurs capacités de nuisance.

M. Philippe Latombe, rapporteur. Les collectivités territoriales réservent-elles toujours un budget à la protection contre la menace cyber ou n'y songent-elles qu'après coup ? Les intégrateurs, souvent sélectionnés par appel d'offres, jouent-ils bien leur rôle ? Angers, par exemple, souffre encore des conséquences d'une attaque, au point qu'elle ne parvient plus à gérer ses horodateurs sur la voie publique.

M. Jérôme Notin. Je me permettrai de remarquer qu'il ne suffit pas à une collectivité territoriale de prendre d'entrée de jeu en compte la cybercriminalité pour y échapper.

Il en va des collectivités territoriales comme des entreprises : leur maturité sur le sujet apparaît corrélée à leur taille. Les plus grandes ont bien conscience du risque, notamment grâce à l'ANSSI. Ce n'est toutefois pas le cas des petites ou moyennes collectivités territoriales, qui ne songent parfois même pas à protéger les données de leurs administrés, n'imaginant pas que celles-ci puissent intéresser les cybercriminels.

Le premier confinement a contribué à une prise de conscience liée à la quantité de collectivités territoriales visées par des rançongiciels. Leurs victimes sont passées de la sixième place sur notre liste de demandes d'assistance en 2019 à la première aujourd'hui. Ces demandes d'assistance ont augmenté de plus de moitié de la part des collectivités territoriales, contre une hausse d'un quart seulement de la part des entreprises et un recul de 85 % de la part des particuliers. Nous assistons donc à un déplacement de la cybercriminalité.

L'été dernier, lors d'une visioconférence, un employé d'une collectivité territoriale m'a remercié, car notre campagne de sensibilisation sur France Télévisions avait enfin convaincu les élus, auxquels il réclamait des fonds depuis des années, de lui allouer un budget cybersécurité.

Une première prise de conscience a donc eu lieu, qu'on ne doit peut-être pas tant à nos actions qu'à la quantité de victimes de cyberattaques. Il nous reste encore du travail et nous nous y attelons. Le plan de relance va permettre d'élever le niveau de sécurité des collectivités territoriales. On ne peut que s'en réjouir.

M. Philippe Latombe, rapporteur. Estimez-vous suffisantes les mesures du plan de relance en matière de cybersécurité ?

M. Jérôme Notin. Les intégrateurs ne jouent pas le jeu : ils n'assurent qu'un service minimum au moindre coût, afin d'obtenir le marché. Ils ne prennent pas assez d'initiatives, alors que les collectivités territoriales sont en droit de les consulter avant la rédaction d'un dossier technique. Ils devraient inciter celles-ci à prendre dès le départ en compte la

cybersécurité, plutôt que de l'ajouter au projet fini à la manière d'une rustine. Je les estime moralement tenus d'alerter les élus sur ce sujet. Il en coûtera à ceux-ci ce que vaut une assurance prémunissant contre les catastrophes.

Le plan de relance prévoit d'allouer 136 millions d'euros à l'ANSSI, dont une partie bénéficiera aux collectivités territoriales, dans la mesure où cette somme nous permettra, entre autres, de mieux sensibiliser à la cybersécurité celles de petite taille. Nous nous efforcerons en 2021 de répondre au plus près à leurs besoins en adaptant à leur intention nos contenus. Nous avons d'ailleurs déjà participé l'an dernier, avec la banque des territoires, à une campagne de sensibilisation des élus au moyen d'un guide. Nous y avons ajouté quatre vidéos illustrant la cybercriminalité par des exemples concrets, comme l'inondation d'un stade de foot suite à une intrusion sur un réseau, ou le dérèglement de feux de circulation obligeant à poster des gendarmes à chaque carrefour.

M. Philippe Latombe, rapporteur. La somme que vous évoquez servira-t-elle directement à protéger les collectivités territoriales ou à dresser une liste de leurs besoins, qui les obligera ensuite à investir ? Beaucoup de collectivités territoriales s'attendent à recevoir de quoi financer leur cybersécurité sans pour autant savoir comment s'attaquer au problème.

M. Jérôme Notin. Nous allons leur indiquer leurs failles et les moyens d'y remédier, sous le pilotage de l'ANSSI. Notre groupement d'intérêt public (GIP) a la chance d'être présidé par M. Guillaume Poupard, le directeur général de l'ANSSI, qui a mis sur pied notre dispositif avec le ministère de l'Intérieur. Nous collaborons au quotidien avec l'ANSSI, à un niveau à la fois stratégique et opérationnel.

M. Philippe Latombe, rapporteur. Les petites et moyennes entreprises (PME) et les très petites entreprises (TPE) se soucient-elles aujourd'hui suffisamment de cybersécurité ?

M. Jérôme Notin. Les grandes entreprises s'en préoccupent assez, grâce à l'ANSSI et à la loi de programmation militaire, par exemple, mais pas les PME. Leurs patrons, à l'instar des élus que j'évoquais tout à l'heure, pensent ne présenter aucun intérêt pour les cybercriminels, puisqu'ils ne possèdent ni fichier clients ni propriété intellectuelle. Les événements de 2020 ont pourtant démontré que la menace cyber touchait tout le monde. Bloquer le réseau d'une PME prend quelques heures à un cybercriminel, qui en retire plusieurs milliers d'euros. Même si peu d'entreprises « passent à la caisse », et tant mieux, une telle opération reste rentable.

Nous œuvrons main dans la main avec des syndicats et des fédérations professionnelles, la confédération des petites et moyennes entreprises (CPME) et le mouvement des entreprises de France (MEDEF). Cette menace réelle n'est toutefois pas encore suffisamment prise en compte. Reconnaissons que notre message manque d'attrait : nous suscitons des craintes et incitons à la dépense. Ceci dit, une telle dépense prépare l'avenir. Nous devons songer que, si la France s'améliore en matière de cybersécurité par rapport à ses voisins, alors les criminels cibleront d'autres pays.

M. Philippe Latombe, rapporteur. Le rôle de sous-traitant de grands groupes assumé par certaines TPE facilite-t-il la diffusion par le haut d'une culture de la cybersécurité ? Je songe à Airbus adressant par exemple à une TPE de Vendée, chargée de fabriquer un morceau d'aile, des plans protégés, amenant ainsi l'entreprise à se moderniser et, du même coup, à se prémunir des cyberattaques.

Pourriez-vous nous communiquer un ordre de grandeur des entreprises victimes de cyberattaques qui, indépendamment de leur taille, paient les rançons ?

M. Jérôme Notin. Quelques grandes entreprises ont bel et bien pris des initiatives hélas encore limitées. La filiale aéronautique et spatiale a lancé l'initiative vertueuse d'Aerospace Valley, à l'impact réel, pour aider les PME critiques de la chaîne d'approvisionnement à mieux se sécuriser.

Cette filière a par ailleurs créé une communauté de confiance : dès lors qu'un des grands donneurs d'ordre a validé le niveau de sécurité d'un prestataire, les autres n'ont plus à s'en préoccuper.

J'ai discuté récemment avec un ami responsable de la sécurité des systèmes d'information (RSSI) chez un intégrateur. Depuis un an, ses tâches se limitent à remplir des dossiers de conformité cyber pour les commerciaux. Chaque donneur d'ordre souhaite en effet désormais qu'un tel dossier accompagne la moindre proposition, comme aux États-Unis. Mon ami RSSI en a perdu de vue son métier.

Songeons aussi au ministère des armées, membre de notre dispositif depuis quelques mois. Il a bien compris que la base industrielle de la technologie de défense constitue la clé de la sécurité et qu'il doit accompagner les entreprises concernées via la direction du renseignement et de la sécurité de la défense (DRSD). Même les PME détentrices d'un savoir-faire spécifique n'ont pas toujours conscience des risques contre lesquels elles doivent se protéger.

M. Philippe Latombe, rapporteur. Le grand public est-il aujourd'hui conscient de ce que représente la menace cyber ? Une culture s'est-elle développée à tous les échelons de la société ?

M. Jérôme Notin. L'ANSSI et les ministères de l'intérieur, des finances, de la justice et des armées, à l'origine de notre dispositif, nous ont confié la mission de lancer une grande campagne de sensibilisation, sur le modèle de celle de la sécurité routière. Je ne doute pas qu'un jour, nous la mènerons à bien. Il ne nous manque que des moyens financiers, mais il suffit d'une volonté politique pour les débloquer.

Il est impératif de se rendre compte que, si le numérique apporte de nombreux bénéfices, son usage requiert par ailleurs une grande vigilance.

Depuis plusieurs mois, des « cybercrapules » appellent des particuliers, soi-disant pour les accompagner dans la création de leur compte professionnel de formation. Leur objectif est en réalité de récupérer le mot de passe associé au profil de la victime pour vider ce compte à l'aide de complices. Pour gagner la bataille, il suffirait que les Français comprennent qu'aucun organisme public ne les contactera jamais en leur demandant leur mot de passe. Le remboursement des victimes a coûté douze millions d'euros à l'État *via* la Caisse des dépôts et consignations (CDC). La justice s'est saisie de l'affaire, cependant il suffirait d'investir un peu pour éviter d'entrer dans des frais de cet ordre.

Dans le même esprit, depuis des années, la fraude à la réparation informatique coûte des millions d'euros tous les mois aux Français qui croient leur ordinateur infecté par un virus, parce que s'ouvre à l'écran une fenêtre les orientant en réalité vers un centre d'appels

vendant de faux antivirus. Je suis convaincu que chaque euro investi dans des actions de sensibilisation en rapporterait à terme plusieurs dizaines.

M. Philippe Latombe, rapporteur. Nous avons auditionné la semaine dernière l'Imprimerie nationale et ATOS au sujet de l'identité numérique, à laquelle pourrait servir de réceptacle la carte d'identité électronique équipée d'une puce. Un code secret lui sera associé, comme à une carte bancaire. Selon vous, nos concitoyens sont-ils suffisamment bien informés des cybermenaces pour éviter tout vol de leur identité ?

M. Jérôme Notin. La CDC a réagi à l'incident relatif au compte professionnel de formation en imposant, en préalable à toute commande de formation, une activation du compte Franceconnect, c'est-à-dire une authentification numérique par un organisme public. Cette excellente réponse technique, opérationnelle, devrait permettre de résoudre les problèmes d'hameçonnage. Reste encore à la généraliser rapidement.

Les cybercriminels, redoutablement imaginatifs, innovent en permanence. En ce moment circule sur les réseaux sociaux une chaîne de messages incitant à leur diffusion auprès d'autres utilisateurs. Leurs auteurs laissent espérer à leurs destinataires que ceux-ci remporteront des entrées gratuites dans un parc d'attractions fêtant son anniversaire, alors qu'ils ne cherchent en réalité qu'à collecter des données personnelles. Beaucoup de jeunes mordent à l'hameçon dans l'espoir de remporter ces invitations et de les offrir à leurs proches. Quelques mois plus tard leur parvient un e-mail émanant en apparence, mettons de la Fnac, de fait très active dans la lutte contre ce type d'arnaques. Ce message, récapitulant les données qu'eux-mêmes ont préalablement communiquées, leur signale la livraison d'une commande qu'ils n'ont bien sûr jamais passée. La possibilité leur est laissée d'en obtenir le remboursement par un simple clic conduisant à une page aux couleurs de la Fnac où leur est alors demandé leur numéro de carte bancaire. Voilà comment les cybercriminels enrichissent progressivement leurs fichiers.

Le recours à l'identité numérique résoudra certains problèmes mais pas celui-là, par exemple.

M. Philippe Latombe, rapporteur. Une anecdote me revient à l'esprit : une chaîne de livraison de repas à domicile, en guise de poisson d'avril, a envoyé des « factures » de livraison de pizzas d'un montant de près de 450 euros. Les clients ayant cru à un piratage vous l'ont-ils signalé ?

M. Jérôme Notin. Non, je n'étais pas au courant.

M. Philippe Latombe, rapporteur. Je m'interrogeais sur l'existence d'un réflexe qui amènerait à vous déclarer systématiquement les situations anormales.

M. Jérôme Notin. En tant que dispositif d'assistance, nous avons pour vocation de fournir de l'aide. Beaucoup déclarent auprès de nous les arnaques dont ils sont victimes. J'y vois l'une des forces de notre dispositif. Ceci étant, comme nous n'employons en tout et pour tout que treize personnes, nous ne communiquons pas trop sur cet aspect de notre rôle. Nous formons une équipe trop réduite pour échanger en direct avec les 1,2 million d'utilisateurs qui se sont connectés à notre plateforme en 2020. Ce chiffre correspond d'ailleurs à une véritable explosion de la fréquentation de notre site pendant le confinement. Quand la forme de cybermalveillance à laquelle nos usagers ont été confrontés n'a pas encore été répertoriée par nos services, ils peuvent la signaler par un message « JNPT » (je n'ai pas trouvé). C'est ainsi

que nous avons eu vent des arnaques au compte professionnel de formation. Nous nous sommes rapidement saisis du problème avec la CDC, qui opère la plateforme de gestion de ces comptes. Cependant, les grands sites privés de commerce ne prennent pas toujours aussi rapidement les devants. Certains ne traitent pas correctement la fraude.

La Française des jeux nous a indiqué que, depuis une dizaine d'années, des particuliers reçoivent un courrier les informant d'un gain à une loterie à laquelle ils n'ont jamais joué. La recrudescence récente du phénomène nous a incités à communiquer sur le sujet prochainement. Jusqu'à une personne sur cinq se laisse prendre en versant parfois des centaines de milliers d'euros à des « avocats » dans l'espoir de récupérer leur gain pourtant fictif.

Expliquer à l'ensemble de nos concitoyens qu'il n'est pas logique qu'ils donnent de l'argent pour percevoir une somme qu'ils auraient gagnée à un jeu auquel ils n'ont pas participé relève d'une action de sensibilisation restant encore à mener.

M. Philippe Latombe, rapporteur. Avez-vous des homologues dans d'autres pays d'Europe ? Si oui, coopérez-vous ? Disposent-ils d'outils qui vous manqueraient ?

M. Jérôme Notin. Nous n'avons pas d'homologues. Tous les États disposent d'une agence nationale équivalente de l'ANSSI et tous mènent des actions de sensibilisation auprès de l'ensemble des publics. En revanche, notre capacité à mettre en relation quasi immédiate des victimes avec des prestataires de proximité en mesure de les aider est unique au monde.

Nous sommes ainsi en mesure d'aiguiller presque tout de suite une collectivité territoriale, mettons en Vendée, vers une entreprise qui se chargera de réinstaller son système d'exploitation après avoir identifié la façon dont s'y sont introduits les attaquants. Je rappelle à ce propos qu'il importe de conserver des preuves des méfaits des cybercriminels avant d'y remédier.

Nous échangeons avec nombre de pays, francophones ou non, proches ou lointains, dans l'idée de leur fournir gratuitement notre outil sous licence libre, pour qu'ils reproduisent notre action sur leur territoire. Derrière notre plateforme œuvre tout un *back-office* qui, à l'aide d'un arbre de décisions, pose des diagnostics et fournit des conseils adaptés aux 45 formes de cybermalveillance que j'évoquais tout à l'heure. Nous proposons aujourd'hui plus de 400 conseils personnalisés. Nous menons presque au quotidien un travail d'adaptation et de reformulation en fonction de ce que nous rapportent les victimes *via* les messages « je n'ai pas trouvé ». Nous complétons régulièrement nos questionnaires et ajoutons de nouvelles formes de cybermalveillance à notre liste.

Les chiffres que nous mettons en avant, les retours de nos utilisateurs et les signalements auprès du parquet d'attaques que n'avaient même pas détectées les services du ministère de l'intérieur, parce que toutes les victimes ne portent pas plainte et qu'il faut de toute façon du temps, après un dépôt de plainte, pour analyser celle-ci et se rendre compte si tel phénomène est isolé ou non, prouvent l'intérêt de notre action. L'adoption d'une taxonomie commune et d'une même définition des incidents de sécurité nous apparaît comme une démarche tout à fait sensée.

Rendre disponible un outil sous forme de logiciel libre requiert un considérable travail, de documentation notamment. J'espère que nous aurons l'occasion de le mener à bien au cours des mois ou des années à venir.

M. Philippe Latombe, rapporteur. Auriez-vous une idée du nombre d'entreprises victimes de rançongiciels qui acceptent de payer ?

M. Jérôme Notin. On cite souvent des proportions allant de 20 à 30 %. Il doit être possible d'améliorer la situation en agissant sur les prestataires qui facilitent le paiement des rançons. Des réflexions sont menées par le Trésor public, le parquet et le ministère de l'intérieur pour leur compliquer la tâche.

J'ai conscience de former là un vœu utopique, mais il faudrait faire passer le message que, si plus personne ne paie de rançon, ce type d'attaque cessera, quitte à ce que les criminels recourent ensuite à d'autres formes de malveillance. En attendant, l'impact de leurs méfaits aura quand même été réduit.

M. Philippe Latombe, rapporteur. Pourriez-vous revenir sur le label que vous avez créé en précisant sa place dans l'écosystème de la cybersécurité ? Que garantit-il exactement ? En quoi se distingue-t-il des autres labels ? Apporte-t-il des assurances complémentaires ? Recoupe-t-il certaines certifications existantes ?

M. Jérôme Notin. Notre label a été créé pour garantir à la victime d'une cyberattaque que l'entreprise vers laquelle elle se tournera possède un niveau d'expertise technique en cybersécurité vérifié. Notre plateforme référence 1 000 prestataires de proximité, allant de petits commerces en régions, en mesure de réinstaller le système d'exploitation d'un particulier exposé à un incident de sécurité, à des Prestataires d'audit de la sécurité des systèmes d'information (PASSI) ou des Prestataires de détection d'incidents de sécurité (PDIS) qualifiés par l'ANSSI.

Quand nous avons créé ce label avec les représentants des prestataires de proximité, notre objectif consistait à garantir leurs compétences en cybersécurité aux PME qui auraient recours à eux. Nous avons établi un référentiel avec l'Association française de normalisation (AFNOR) en vue de réaliser un audit des prestataires. Cet audit se base sur une documentation, d'une part, de leurs réponses aux incidents de sécurité et, d'autre part, de leurs actions de sécurisation auprès de leurs clients. Un examen technique d'une vingtaine de minutes comportant 30 à 40 questions le complète. L'obtention du label dépend de la note obtenue.

Les représentants de la profession nous ont signalé la nécessité d'évaluer leur capacité à sécuriser des systèmes, au-delà de leur aptitude à gérer les incidents. Nous avons ainsi identifié sur l'ensemble du territoire 55 entreprises en mesure d'éviter aux PME et aux collectivités territoriales de tomber dans le piège d'une cyberattaque. Nous ambitionnons de faire passer leur nombre à 200 voire à 400. Nos entreprises et nos collectivités territoriales doivent pouvoir s'appuyer sur un réseau de prestataires de confiance capables de leur fournir une solution rapide aux incidents, mais aussi d'élever globalement le niveau de sécurité cyber.

M. Philippe Latombe, rapporteur. Les entreprises se prémunissent-elles suffisamment contre les risques de cyberattaques ? Que proposent en ce domaine les compagnies d'assurance et qu'en coûte-t-il ? Utilisent-elles les protections contre la cybercriminalité de la même manière qu'elles se sont servies des portes blindées, c'est-à-dire comme d'un levier de diffusion, en l'occurrence d'une culture de la cybersécurité ? Autrement dit : les compagnies d'assurance refusent-elles de couvrir les entreprises et collectivités territoriales mal protégées ? Leur imposent-elles des tarifs supérieurs ?

M. Jérôme Notin. Les compagnies d'assurance disposent là d'un formidable levier. Nous nous réjouissons d'ailleurs de compter la fédération française de l'assurance parmi les membres fondateurs de notre GIP. Trois assureurs nous ont rejoints depuis. Nous travaillons avec eux sur la partie « observatoire » du dispositif. Il leur faut des chiffres précis pour concevoir des polices d'assurance efficaces.

Des progrès restent à réaliser, tant de l'offre elle-même que de l'adhésion des victimes potentielles. Nous avons besoin, d'un côté, d'une offre cyber adaptée au marché et, de l'autre, de clients conscients que les assureurs ne couvriront que les risques résiduels. Notre label intéresse de ce fait aussi les assureurs, désireux de s'appuyer sur des prestataires capables d'évaluer le niveau de cybersécurité de leurs clients. Une assurance cyber bien conçue ne coûte que quelques centaines d'euros à une PME.

Nous demandons en somme aux assureurs de nous aider à les aider. Nous ignorons quels chiffres au juste ils souhaitent connaître. Nous œuvrons en outre avec eux à déterminer comment communiquer de manière anonyme sur le coût des cyberattaques et le temps d'immobilisation potentiel des systèmes pour qu'une offre adaptée voie le jour et que les entreprises se prémunissent de leur côté contre les risques les plus courants.

M. Philippe Latombe, rapporteur. Les assurances tentent-elles, non sans opportunisme, de conquérir un nouveau marché ou se rendent-elles compte qu'elles risquent de perdre des clients si elles s'avèrent incapables de protéger les entreprises de leur portefeuille, à présent numérisées et, partant, plus vulnérables, car exposées à des risques jusque-là inexistants ?

M. Jérôme Notin. Leur démarche participe sans doute des deux approches que vous évoquez, et peut-être plus de la première mais, en un sens, peu importe, d'autant que la distinction n'apparaît pas nette.

Le marché des polices cyber représente 40 millions d'euros, soit une part infime du marché des assurances. L'apparition, dans les prochaines années, de véhicules autonomes entraînera une diminution du chiffre d'affaires des assureurs, ces véhicules présentant des risques d'accident moindres, sauf, évidemment, si des pirates prennent le contrôle de l'ensemble du système de pilotage. Il semble donc logique que les assureurs compensent le manque à gagner sur les polices d'assurance automobile en proposant de couvrir les risques cyber. Tant qu'on observe une adéquation entre la nouvelle offre et les besoins, on peut considérer cette évolution comme vertueuse.

Il faut en tout cas que des assureurs couvrent le risque cyber, quelle que soit leur motivation. J'espère que notre observatoire nous permettra sous peu de fournir le nombre exact des PME en France incapables de se relever d'attaques cyber. Le maire d'Angers a eu l'intelligence de communiquer sur la situation de sa ville, mais il n'est pas le seul confronté à ce type de problème.

Un directeur général dans une commune importante me confiait récemment que, depuis une attaque en novembre, son service ne fonctionnait plus qu'au cinquième de sa capacité nominale, l'empêchant de servir les administrés. La création de polices d'assurance adaptées pourrait remédier à de telles difficultés en imposant par exemple de réaliser des sauvegardes déconnectées.

M. Philippe Latombe, rapporteur. L'incendie d'OVH a montré que bien peu d'entreprises et de collectivités hébergées sur leur *cloud* disposaient d'un plan de reprise d'activité (PRA) ou d'un plan de continuité d'activité (PCA), pourtant à la base de toute protection d'un système informatique. Cet incident a contraint certains hôpitaux incapables de se passer de l'informatique à fonctionner en mode dégradé.

Les organisations professionnelles, dont certaines font partie de votre GIP (la CPME et le MEDEF), relaient-elles aujourd'hui l'information auprès de leurs adhérents ? La fonction publique, dans son versant hospitalier décentralisé notamment, est-elle suffisamment avertie du risque cyber ? A-t-elle assez conscience de sa vulnérabilité pour vous solliciter afin de prendre les mesures adéquates ?

M. Jérôme Notin. L'actualité a montré l'absence totale de scrupules des cybercriminels, n'hésitant pas à entraver le fonctionnement d'un établissement de santé, quitte à empêcher le personnel soignant d'assurer sa mission, à la seule fin de récupérer de l'argent. Cela, les hôpitaux l'ont compris.

Le problème qui se pose est celui de la dette technique des collectivités territoriales, à présent tenues de compenser leur manque d'investissement en cybersécurité. Tant qu'elles n'y seront pas parvenues, elles resteront vulnérables. Par chance, la France dispose d'une agence nationale de la santé, et l'ANSSI réalise un travail fabuleux d'accompagnement après les incidents. Je garde confiance en notre capacité à rattraper rapidement notre retard, grâce au plan de relance qui s'est concentré sur le domaine hospitalier.

Dès le début du premier confinement, les fédérations professionnelles et le MEDEF nous ont contactés, parce que leurs adhérents ne savaient pas comment mettre en place le télétravail de manière sécurisée. Nous leur avons très vite fourni des conseils dans un article largement relayé sur la mise en place du télétravail en situation de crise.

En tant que plateforme « .gouv.fr », nous nous sommes octroyé le droit, par souci de pragmatisme, de rappeler, en cas d'utilisation d'un ordinateur personnel à des fins professionnelles, quelques principes de base, tels que la mise à jour d'un antivirus, l'installation de pare-feu locaux ou d'un VPN.

Le MEDEF, la CPME, la fédération Syntec et la fédération des entreprises du bureau et du numérique (EBEN) se sont empressés de relayer cet article, destiné à l'origine aux patrons de PME, preuve d'une véritable demande de leur part. La CPME, qui vient d'engager quelqu'un d'extrêmement volontaire en matière de cybersécurité, se montre depuis longtemps très active dans notre dispositif.

Les fédérations assument donc leur rôle. Reste à savoir si leurs adhérents saisissent bien le message.

Mon contact à la CPME m'a confié que, lorsque, deux ou trois ans plus tôt, il proposait aux adhérents locaux des formations à la cybersécurité, celles-ci ne suscitaient aucun intérêt. Aujourd'hui, à l'inverse, la cybersécurité apparaît bien comme le premier sujet de préoccupation des patrons de PME.

La prise de conscience du risque s'améliore, or elle marque une première étape indispensable avant d'entreprendre le nécessaire pour s'en prémunir.

M. Philippe Latombe, rapporteur. La formation des experts en cybersécurité et des RSSI vous semble-t-elle aujourd'hui d'un niveau satisfaisant ?

M. Jérôme Notin. Les formations actuellement dispensées en France, en informatique en général et en cybersécurité en particulier, sont d'un très bon niveau. Les écoles produisent des diplômés aux profils parfaitement adaptés aux besoins. Ceci dit, ils sont loin d'être assez nombreux.

Le manque ne porte pas seulement sur les ingénieurs aux compétences pointues mais aussi sur les techniciens. L'idée reste prégnante en France qu'un métier technique est « sale ». Il nous faudrait plus de personnel intermédiaire de niveau bac +2 qui mette les mains sur le clavier pour opérer directement les infrastructures.

Les écoles d'ingénieurs, qui préparent leurs étudiants à devenir chefs de projet après deux ou trois ans de carrière, leur annoncent qu'ils oublieront dès lors l'aspect technique de leur métier, ce que je trouve scandaleux. Chacun doit pouvoir continuer à s'occuper de questions techniques, quel que soit son âge. Prétendre qu'il faudrait renoncer à la technique pour devenir RSSI n'a pas de sens et relève selon moi d'une déformation française, dégradante, qui plus est, pour l'image de la technique. D'autant que celle-ci correspond quand même à un besoin fondamental de l'entreprise, au même titre que sa stratégie ou son organisation. Il est nécessaire que des personnes compétentes administrent les réseaux au quotidien et vérifient les règles des pare-feu.

M. Philippe Latombe, rapporteur. Selon vous, qui devrait former des techniciens ? Des instituts universitaires de technologie (IUT) ?

M. Jérôme Notin. On pourrait valoriser les brevets de technicien supérieur (BTS). Ayant moi-même quitté l'université depuis un certain temps, j'ai quelque peu perdu de vue l'organisation des études supérieures. Je songeais à des formations de niveau bac+2 ou bac+3. En France perdure une culture de l'élitisme, qui explique ce défaut de personnel qualifié de niveau intermédiaire.

Il faut aussi se dire qu'un ingénieur peut encore « s'amuser » à 45 ans en s'occupant de technique. L'état d'esprit qui prévaut, et que je ne suis malheureusement pas en mesure de changer, me paraît dommageable. Des étudiants frais émoulus d'une école d'ingénieurs m'expliquaient, voici quelques années, qu'un emploi de consultant leur semblait plus noble qu'un poste d'administrateur de réseaux. Je ne partage pas ce point de vue.

M. Philippe Latombe, rapporteur. Que pensez-vous du futur campus cyber ? Comment concevez-vous son rôle et son futur impact ? Le voyez-vous comme une belle vitrine à même d'attirer des talents, comme un dispositif efficace qu'il conviendra de généraliser ? Le jugez-vous trop centralisé, même s'il est prévu qu'il essaime en région ? Faudrait-il le dupliquer au niveau européen ?

M. Jérôme Notin. J'y vois avant tout une opportunité extraordinaire. Sur le papier au moins, il m'apparaît comme un dispositif fabuleux. Réunir en un même lieu les acteurs industriels, universitaires, étatiques, les *start-up* et les investisseurs, permettrait à la France de réaliser, en matière de cybersécurité, les formidables progrès dont elle a besoin.

Cela étant, il faut, pour que ce campus réussisse, que tout le monde joue le jeu, ce qui ne s'annonce pas simple. Michel Van Den Berghe, qui porte le projet, parvient aujourd'hui, ce

dont je me réjouis d'ailleurs, à faire passer à de grands groupes industriels concurrents le message qu'ils travailleront ensemble à des projets communs.

De grands groupes industriels du secteur de la défense mettent pour l'heure au point, indépendamment les uns des autres, des dispositifs de sécurité spécifiques destinés à renforcer un système d'exploitation commun. S'ils mutualisaient leurs ressources en personnel, en s'adjoignant le concours d'un universitaire, autrement dit s'ils œuvraient de concert, ils gagneraient en efficacité. Or tel est l'objectif du campus.

Notre GIP aura la chance de rejoindre ce campus. Notre observatoire de la menace se construira en son sein. Si j'ai pleine confiance en ce projet, je doute quand même un peu de la capacité des industriels à travailler ensemble. L'ANSSI sera heureusement très présente. Il faudra peut-être plus de temps qu'on ne l'imagine aujourd'hui à ce cyber campus pour porter ses fruits.

Je vous livrerai mon avis personnel sur ses déclinaisons régionales. Il existe déjà de remarquables initiatives à Saint-Quentin-en-Yvelines, dans le Nord et la région Provence-Alpes-Côte d'Azur (PACA). Des déclinaisons régionales du campus réalisant un maillage du territoire permettraient de franchir une étape cruciale.

Nous répétons depuis tout à l'heure que les principales victimes de la cybermalveillance ne sont autres que les PME et les collectivités territoriales, par nature ancrées dans les territoires. Disposer dans le tissu économique local de structures en mesure de déployer des technologies cyber adaptées nous donnera les moyens de réaliser en cinq ans des progrès tels que 2021 nous apparaîtra, avec le recul, comme une période moyenâgeuse en matière de cybersécurité.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous aborder d'autres sujets que nous aurions omis ?

M. Jérôme Notin. Nous avons consacré beaucoup d'énergie à la rédaction de notre rapport d'activité, que nous allons publier dans quelques jours. Fruit d'un travail collectif, il récapitule des chiffres relatifs à la cybermenace, son analyse et ses tendances les plus récentes. N'hésitez pas à consacrer un peu de temps à sa lecture. J'invite enfin ceux qui assistent à cette audition à nous suivre sur les réseaux sociaux et à s'inscrire à notre lettre d'information.

M. Philippe Latombe, rapporteur. Pourriez-vous nous faire parvenir ce rapport ? Nous l'ajouterons en annexe et disposerons ainsi de plus amples éléments pour nourrir notre réflexion.

M. Jérôme Notin. Je n'osais pas vous le proposer, mais je vous le transmettrai avec plaisir.

M. Philippe Latombe, rapporteur. Je vous souhaite bon courage pour la création de l'observatoire, qui devrait en effet permettre de mieux suivre l'évolution de la cybermenace d'un point de vue aussi bien qualitatif que quantitatif.

La séance est levée à 10 heures 20.

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 neuf heures trente

Présents. – MM. Éric Bothorel, Philippe Latombe, Jean-Luc Warsmann

Excusée. – Mme Frédérique Dumas