ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Mardi
13 avril 2021
Séance de 11 h 15

Compte rendu n° 58

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Arnaud Dechoux, responsable des affaires publiques « Europe », de la société Kaspersky

La séance est ouverte à 11 h 15.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos auditions consacrées aux enjeux du cyber, en présence de M. Arnaud Dechoux, responsable des affaires publiques de la société Kaspersky France.

Notre mission s'intéresse au sujet de la cybersécurité et de la cyberdéfense, qui constituent le cœur de la souveraineté numérique, entendue dans le sens le plus fondamental. Nous avons souhaité vous entendre comme représentant d'une société multinationale russe, spécialisée dans la sécurité des systèmes d'information, et connue évidemment pour sa solution antivirus. Nous sommes intéressés par votre regard et celui de votre société, en tant qu'acteur n'appartenant pas à l'Union européenne, sur la préoccupation croissante des États membres de celle-ci vis-à-vis de l'enjeu de souveraineté numérique. Nous aurons également l'occasion, je l'espère, d'aborder votre manière de voir l'actualité cyber européenne. Vous avez organisé le 23 mars dernier un échange sur le sujet avec plusieurs acteurs importants, dont M. Guillaume Poupard, le directeur général de l'agence nationale de sécurité des systèmes d'information (ANSSI), M. Bart Groothuis, eurodéputé et rapporteur de la directive NIS2. J'espère que vous pourrez nous en dire un mot.

M. Philippe Latombe, rapporteur. Je souhaite évoquer trois sujets.

La première question est rituelle dans cette mission et porte sur la façon dont vous appréhendez la notion de souveraineté numérique. Dans nos différentes auditions, nous avons entendu une grande diversité de définitions. Je voudrais donc savoir ce que recouvre, sous l'angle cyber, ce concept que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle. Comment vous positionnez-vous face au souhait de certains États membres de privilégier des solutions de sécurité européennes pour des raisons de souveraineté ?

En second point, je voudrais que nous échangions sur le secteur de la cybersécurité. Quel est votre positionnement sur le marché des antivirus, et son actualité en Europe et dans le monde ? Comment faites-vous en sorte de rester à l'état de l'art face à l'évolution des menaces ? J'aimerais que vous partagiez votre regard sur l'évolution de la menace, tant en ce qui concerne sa nature que ses modalités. Très concrètement, comment les attaques subies par vos clients ont-elles évolué ? Ceux-ci avaient-ils renforcé leur protection numérique pendant la crise sanitaire ? Comment inciter les entreprises à mieux se protéger dorénavant, afin de limiter autant que possible les conséquences d'éventuelles atteintes à leurs systèmes d'information ?

Enfin, j'aimerais revenir sur la question de la protection des données personnelles, qui est un sujet majeur en Europe. Comment percevez-vous cet impératif, en tant qu'acteur non européen ? Comment garantissez-vous la sécurité des données de vos clients, alors que certains vous accusent d'avoir favorisé l'installation de *backdoors* au sein de systèmes informatiques au profit de la Russie ?

Je rejoins M. le président pour conclure sur l'actualité cyber européenne, sur laquelle nous aimerions aussi évidemment vous entendre.

M. Arnaud Dechoux, responsable des affaires publiques « Europe », de la société Kaspersky. Si vous me le permettez, je voudrais présenter très rapidement Kaspersky, pour expliquer qui nous sommes, ce que nous faisons et ce que nous ne faisons pas. L'entreprise a été fondée en 1997 par Eugène Kaspersky, qui reste aujourd'hui son président-directeur général et son propriétaire. Avec un chiffre d'affaires d'environ sept cents millions de dollars, Kaspersky est la première entreprise privée de cybersécurité au niveau mondial. Elle emploie environ quatre mille salariés dans le monde, dont plus d'un tiers en R&D. L'entreprise a l'originalité d'être une multinationale d'origine russe, dans un secteur où les grands acteurs sont souvent d'origine anglo-saxonne. L'Europe constitue aujourd'hui, de loin, notre première zone d'activité : 40 % environ de notre chiffre d'affaires sont aujourd'hui réalisés en Europe. Nous attachons donc beaucoup d'importance aux considérations européennes, entre autres sur les sujets de souveraineté numérique.

Kaspersky est initialement connu pour son moteur antivirus très efficace, mais est aujourd'hui bien autre chose. Nous avons deux segments d'activité. En premier lieu, le segment grand public constitue environ 50 % de notre activité : il s'agit de la protection des ordinateurs, de gestionnaires de mots de passe, de réseaux privés virtuels (VPN) ou encore de solutions de contrôle parental. La deuxième moitié concerne les services aux entreprises et organisations ; environ deux cent soixante-dix mille organisations sont clientes de Kaspersky, de la très petite entreprise (TPE) ou petite et moyenne entreprise (PME) à la multinationale, en passant par de nombreuses organisations publiques. Nous parlons en l'occurrence de solutions de protection des postes de travail, mais aussi de sondes réseau ou de protections pour le milieu industriel, qui est également très ciblé aujourd'hui par les cyberattaques, d'outils de protection des objets connectés, ou encore de chiffrement des infrastructures *cloud*, mais aussi de programmes de sensibilisation à la cybersécurité.

La dernière activité sur laquelle je voulais insister est celle des services *threat intelligence*, autrement dit de renseignement cyber sur les menaces avancées. Très concrètement, ce sont des flux d'informations à destination des agents de cybersécurité, des grandes entreprises, des intégrateurs, qui possèdent en interne des *computer emergency response teams* (CERT) ou des *security operations centers* (SOC), c'est-à-dire des équipes chargées de réaliser de la veille cyber. L'objectif pour ces acteurs est de mieux connaître la menace, de mieux s'y préparer et de mieux gérer les risques cyber. Chez Kaspersky, cette activité est gérée par une équipe appelée *Global research analysis team* (GReAT) : quatre chercheurs en France sont spécialisés sur ces sujets.

Nous comptons quatre cents millions d'utilisateurs dans le monde pour nos différents services. C'est précisément cette présence internationale qui nous permet de suivre en temps réel l'évolution des cybermenaces dans les différents pays. Les utilisateurs qui le souhaitent nous remontent, après avoir accepté cette modalité par un système d'*opt-in,* des données de télémétrie, qui permettent d'analyser les fichiers malveillants auxquels ils sont confrontés, en particulier ceux que nous ne connaissons pas encore. L'objectif est d'analyser ces derniers pour mieux les identifier à l'avenir.

Kaspersky emploie 70 personnes en France, où elle existe depuis une quinzaine d'années. L'entreprise est membre de la plateforme Cybermalveillance depuis 2017, acteur que vous avez auditionné et qui nous semble extrêmement important pour sensibiliser et instaurer une véritable culture d'hygiène numérique parmi les citoyens et les petites entreprises. L'entreprise est également signataire, depuis 2018, de l'Appel de Paris pour la confiance et la sécurité du cyberespace. Dans ce cadre, nous codirigeons depuis quelques

mois avec le Cigref l'un des groupes de travail mis en place par le ministère de l'Europe et des affaires étrangères, pour apporter des outils concrets aux signataires de l'Appel.

L'un des maîtres mots de Kaspersky, en France comme dans le monde, est la transparence, pour répondre à des risques, fussent-ils théoriques, et à un éventuel manque de confiance, tel qu'il a pu exister. L'entreprise a mis en place depuis 2017 une initiative mondiale de transparence (*global transparency* initiative, GTI), qui nous semble l'un des programmes les plus avancés, voire le plus avancé dans le domaine. Il s'agit également d'une réponse aux enjeux de souveraineté de nos clients. Nous pourrons y revenir si vous le souhaitez.

Je vous propose de revenir sur quelques évolutions récentes du paysage des cybermenaces, notamment du fait de la crise sanitaire, mais non uniquement.

Kaspersky distingue classiquement trois types de menaces. Le premier est celui de la cybercriminalité traditionnelle, qui représente environ 80 % du volume des fichiers que nous détectons. Ces menaces sont en réalité assez faciles à détecter, et se traitent automatiquement. Il s'agit souvent de criminels traditionnels qui se sont mis au cyber, en considérant qu'il procédait d'un bon *business model*, avec des risques limités.

Le deuxième étage est celui des menaces ciblées, qui visent principalement des organisations. Elles représentent environ 20 % du volume total des détections, et sont déployées par des groupes d'attaquants beaucoup plus spécialisés, organisés, voire très professionnels. Les rançongiciels en sont un très bon exemple.

La dernière catégorie est celle des cyberarmes, déployées par des groupes étatiques ou paraétatiques ; elles ne représentent que 0,01 % du volume, mais ces attaques sont très visibles. Elles peuvent avoir des objectifs d'espionnage ou de sabotage, voire des visées financières dans certains cas très précis – je pense notamment aux attaques de la Corée du Nord cherchant à obtenir des devises. Dans cette dernière catégorie, la question de l'attribution des cyberattaques est une tâche très complexe.

Nous constatons une augmentation constante des cyberattaques depuis la création de Kaspersky. En 1994, on détectait un nouveau virus ou fichier malveillant par heure : le rythme est passé à un virus par minute en 2006, un virus par seconde en 2011. Les chiffres continuent à augmenter : 350 000 virus étaient détectés chaque jour en 2019 ; en 2020, en partie à cause de la situation sanitaire et du confinement, on atteignait 428 000 virus par jour, soit une progression de 25 % des détections en un an. La situation liée à la covid-19 et aux restrictions de déplacements a entraîné une augmentation de certains types de cyberattaques. Je pense notamment aux attaques de services d'accès à distance (*remote desktop protocol*, RDP) ou aux rançongiciels ciblés sur les établissements de santé, par exemple. Nous essayons néanmoins de relativiser ce constat en observant qu'il n'y a pas eu de progression exponentielle, mais une progression stable des attaques. La progression de ces derniers mois est également due à l'élargissement de la surface d'attaque : augmentation du temps passé sur Internet, du travail à distance, avec des équipements souvent moins bien protégés que ceux des entreprises, et recours à des ressources éducatives en ligne. Dans ce dernier cas, nous avons vu d'autres types d'attaques, comme celles par déni de service (DDoS), qui se sont beaucoup développées lors du premier confinement en mars dernier, et la semaine dernière encore en France. Ceci est dû aussi bien sûr au développement des objets connectés.

Pour finir, je voudrais revenir sur plusieurs tendances récentes que nous avons observées.

La première est le développement des attaques sur mobile. On protège aujourd'hui largement son ordinateur, mais on pense rarement à son smartphone, qui contient pourtant toute notre vie numérique. Il s'agit selon nous d'un axe de progrès important.

L'explosion des rançongiciels ciblés, qui visent beaucoup les entreprises, collectivités territoriales et établissements de santé, est une autre tendance majeure. Nous avons constaté au cours des deux dernières années un transfert des rançongiciels non discriminés, visant des dizaines de milliers de personnes, dont beaucoup de simples utilisateurs, à un ciblage ces derniers mois des grandes organisations, en particulier les grandes entreprises, qui ont les moyens de payer et sont plus susceptibles de le faire, car la perturbation de l'activité risque de fortement impacter la vie de leurs utilisateurs.

Un troisième phénomène est la structuration importante et la professionnalisation de l'écosystème cybercriminel. C'est notamment le cas pour les rançongiciels dont nous venons de parler. On a souvent l'impression que l'entreprise a affaire à un seul groupe de hackers, mais elle est en réalité confrontée à une dizaine de parties prenantes distinctes, l'un des groupes se chargeant du développement du rançongiciel, le deuxième fournissant les accès, un troisième se chargeant du contact client (certains faisant même appel à un standard téléphonique pour faire des relances), un autre encore se chargeant du blanchiment d'argent. Il s'agit aujourd'hui d'un écosystème très complexe, très structuré, et contre lequel il est d'autant plus difficile de lutter. C'est pour cette raison que la collaboration nous semble importante.

Enfin, les attaques dites par chaîne d'approvisionnement (*supply chain)* visent la chaîne logistique, et consistent souvent à passer par un sous-traitant pour atteindre la cible finale. Un exemple a fait beaucoup de bruit, depuis le mois de décembre 2020, avec l'attaque, sans doute liée à de l'espionnage, de Sunburst sur les produits SolarWinds, qui a notamment affecté des entités américaines. Sur ce type de sujets, de même que pour les attaques d'infrastructures critiques, nous avons constaté une montée en compétences des cyberattaquants, et un activisme accru de certains acteurs que l'on ne voyait pas auparavant. Je pense en l'occurrence à des États, qui ont développé leur capacité cyber et montent en compétences sur les cyberarmes, éventuellement en achetant des outils sur les marchés noirs à d'autres acteurs.

En conclusion, je dirais qu'au vu de tous ces enjeux, il est essentiel de promouvoir la cybersécurité par conception, voire la cyberimmunité des produits. C'est un concept que nous essayons de promouvoir, et qui consiste à redémarrer sur la base de systèmes d'exploitation totalement sécurisés. Beaucoup de systèmes de contrôle industriel (*supervisory control and data acquisition*, SCADA) ont été *designés* il y a des dizaines d'années et ne sont plus au niveau. Ils imposent de redémarrer de zéro. La sécurité par conception, le partage d'informations et les partenariats publics-privés sont essentiels.

Cyber Malveillance et le Cyber Campus, que vous avez je crois auditionnés, nous semblent des acteurs clefs dans ce domaine. La collaboration est le seul moyen qui nous permettra de répondre efficacement aux cybermenaces en constante évolution.

M. Philippe Latombe, rapporteur. Selon vous, qu'est-ce que la souveraineté numérique ? Vous êtes Européen, mais travaillez pour une société non européenne : comment

voyez-vous cette notion monter ? Progresse-t-elle assez vite pour être perçue comme un enjeu, par exemple un frein, pour Kaspersky ?

M. Arnaud Dechoux. Nous sommes nés en Russie, mais pas un acteur tout à fait russe aujourd'hui. La société est immatriculée à Londres. Kaspersky France est une structure totalement française.

M. Philippe Latombe, rapporteur. Vous restez non européens.

M. Arnaud Dechoux. Ce n'est effectivement plus un bon argument, sinon pour les aspects culturels.

La notion de souveraineté numérique est évidemment un sujet extrêmement important. Un acteur international comme Kaspersky a pu observer la montée de ces enjeux de souveraineté partout dans le monde. Le terme de souveraineté numérique n'est pas forcément celui qui est utilisé ailleurs, et l'on peut nous demander, en Russie ou dans d'autres pays, ce que signifie exactement cette notion, qui est surtout utilisée en Europe.

Le concept se décline selon nous à trois niveaux – la souveraineté des États, celle des organisations et celle des utilisateurs ou citoyens, avec des enjeux distincts. Pour ce qui est de la souveraineté des solutions et des services numériques, nous pensons à plusieurs grands principes. Sans surprise, elle implique pour les utilisateurs le contrôle complet de leurs données (savoir où elles vont, pouvoir choisir avec qui elles sont partagées). Du point de vue du commanditaire, que ce soit un État ou une entreprise, elle renvoie à la maîtrise et à la connaissance des solutions informatiques utilisées. Le Cigref soulignait que les outils informatiques sont censés faire ce qu'ils doivent faire, et rien d'autre. Nous adhérons pleinement à cette définition. Cela passe beaucoup par la transparence des éditeurs des solutions de cybersécurité ou d'autres solutions. La possibilité d'auditer le code source, que nous avons essayé de promouvoir par notre initiative mondiale de transparence, nous semble à cet égard un axe clef.

Vous avez mentionné le fait d'être ou non européen. Cela ne vous surprendra pas, mais la souveraineté doit selon nous, en vertu des valeurs européennes, passer par la libre concurrence et la non-discrimination. À ce titre, la nationalité d'origine de l'éditeur ne nous semble pas un élément pertinent. On peut bien sûr en tenir compte, mais elle doit être associée à d'autres facteurs, comme la confiance en l'éditeur, sa structure capitalistique, sa manière de gérer les données, l'assurance que l'on peut avoir que les données ne sont pas transmises.

Le dernier principe qui nous semble important pour qu'un État ou une entreprise puissent assurer leur souveraineté numérique est le fait que les prestataires de services ou de solutions respectent les valeurs européennes et coopèrent avec les autorités. Ce point est particulièrement important dans le secteur de la cybersécurité en particulier, où l'on voit beaucoup de coopérations entre les entreprises et les forces de l'ordre, pour des investigations conjointes ou pour du partage d'expertise plus généralement avec la société civile et le monde académique.

Pour ce qui est des opérations conjointes, citons l'exemple de la saisie du serveur de *command and control* d'un groupe cybercriminel par des forces de police : ces dernières peuvent faire appel à une société comme Kaspersky pour aider à l'analyse du serveur afin d'essayer de remonter à la source et de trouver des clefs de déchiffrement de rançongiciels. Une initiative a très bien fonctionné sur le sujet, la plateforme No More Ransom, lancée en

2016 par la police néerlandaise, Europol, Kaspersky et McAfee. Cette plateforme réunit aujourd'hui plus de cent soixante parties prenantes, dont beaucoup de polices européennes. La police et la gendarmerie françaises en font partie. L'objectif est de donner des clefs de déchiffrement gratuitement aux personnes victimes de rançongiciels. Cette plateforme est bien sûr moins utile aujourd'hui, puisque les rançongiciels sont désormais beaucoup plus ciblés et complexes qu'auparavant. Il s'agit en tout cas d'un bon exemple de partenariat qui fonctionne.

En conclusion sur la souveraineté numérique, la non-dépendance vis-à-vis d'un fournisseur unique nous paraît un élément important pour un État ou une entreprise. En l'occurrence, la cybersécurité est un secteur relativement fragmenté, à la différence de celui de l'hébergement *cloud*. Il existe de nombreuses solutions, européennes ou non, permettant à un État de choisir au mieux et de ne pas être pieds et poings liés avec un éditeur. La question n'est pas tout à fait la même.

M. Philippe Latombe, rapporteur. La question n'est effectivement pas tout à fait la même entre le *cloud* et la cybersécurité, mais percevez-vous chez vos clients une demande de plus en plus importante de solutions de type souveraines ? Cela fait-il partie des critères mis en avant, et recevez-vous des questions sur le sujet, ce qui vous obligerait à le déminer, sachant que vous n'êtes pas directement européen ? Une campagne a été menée disant que Kaspersky avait ouvert des *backdoors* pour les services russes. Cette situation vous pénalise-t-elle ? Quel est votre état d'esprit sur le sujet ?

M. Arnaud Dechoux. Je vous remercie de cette question très pertinente. Notre réponse est tout à fait positive. Nous percevons chez tous les clients, en particulier les grandes entreprises ou les intégrateurs qui revendent leurs services à d'autres entreprises, la montée de ces enjeux de souveraineté. Je ne saurais pas vous dire si le sujet est formalisé de manière juridique dans les appels d'offres, mais la question nous est systématiquement posée. Cette question est d'ailleurs peut-être moins posée à des acteurs d'origine anglo-saxonne.

En 2017, Kaspersky a été accusé, selon nous de façon complètement infondée, d'avoir installé des *backdoors* ou transmis des informations récoltées. Le manque de confiance généré n'aide pas la communauté à mieux se protéger. Nous pensons qu'il faut rétablir la confiance, ce qui passe par de la collaboration, pour mieux se protéger contre ces cyberattaques, qui peuvent venir de l'étranger, et en tout cas pas de la porte d'à côté.

Nous avons essayé de répondre au manque de confiance à travers une initiative lancée en 2017, qui répond également aux enjeux de souveraineté, même si le terme n'existait pas encore à l'époque.

Le premier socle est la relocalisation du cœur de l'infrastructure de stockage et de traitement des données de nos clients en Suisse. Les données étaient auparavant hébergées dans des *datacenters* localisés à Moscou : la Suisse a été choisie, car elle est un symbole d'indépendance, et parce que nous possédions déjà des *datacenters* à proximité de Zurich. Toutes les données des clients européens y ont été relocalisées dans un premier temps. Nous y avons ensuite, en 2018, 2019 et 2020, transféré celles des clients nord-américains et d'une partie importante des pays asiatiques. De nombreuses réticences ont été soulevées en interne par des personnes qui estimaient que la localisation des données n'était pas un facteur pertinent pour la cybersécurité, mais les mentalités ont ensuite changé. Nous avons vu tout l'intérêt de ce genre d'approche, que nous poursuivrons.

Le deuxième pilier est l'ouverture de centres de transparence. Des centres ont été adossés au *datacenter* de Zurich, nous en avons également ouvert à Madrid, au Brésil, en Malaisie et depuis peu au Canada. L'objectif est de permettre à nos clients et partenaires, qui sont souvent des agences de cybersécurité nationales, de venir auditer notre code source, et toutes les mises à jour des solutions. Vous évoquiez l'accusation de mise en place de *backdoors* : cela peut notamment se faire par des mises à jour. Pour un client, entreprise ou autre, la possibilité d'auditer l'ensemble de l'historique des mises à jour nous semble un facteur capital. Nous ne sommes pas la seule entreprise à avoir mis en place ce type de dispositif de transparence, mais le nôtre est particulièrement avancé. Je vous mentirais si je vous indiquais que des centaines d'entreprises viennent auditer notre code source : vingt à trente parties prenantes sont venues le faire depuis l'ouverture des centres de transparence. Il faut beaucoup de ressources pour auditer complètement les solutions informatiques, même si elles restent plus faciles à auditer qu'une infrastructure 5G, qui représente des millions de lignes de code. En tout cas, cette possibilité existe, et il s'agit d'une preuve de confiance importante pour les entreprises ou les autorités publiques.

L'avant-dernier pilier est l'audit des processus internes par des tiers que sont les grands cabinets d'audit reconnus mondialement, lesquels passent en revue le développement et les bases des règles de détection des menaces, pour s'assurer qu'ils sont protégés de toute modification non autorisée, par de robustes mesures de sécurité. Un certain nombre de certifications existent dans le domaine de la cybersécurité, notamment la norme ISO 27001, que nous avons obtenue auprès d'un organisme autrichien.

Le tout dernier pilier, qui me semble également intéressant pour votre question relative à la souveraineté numérique, est la gestion des vulnérabilités. Nous en retrouvons dans à peu près toutes les solutions informatiques, en particulier celles qui ont été conçues il y a très longtemps. Les solutions de Kaspersky n'échappent pas à la règle. Nous avons mis en place un dispositif clair pour faire en sorte que les chercheurs puissent auditer nos solutions, sans être attaqués en justice – comme cela s'est fait dans d'autres entreprises. Nous avons également publié nos principes éthiques de gestion des vulnérabilités que nous trouvons dans les solutions d'autres entreprises. Un certain nombre d'étapes doivent être suivies : il faut bien sûr prévenir en premier lieu l'entreprise victime, faire en sorte qu'elle puisse corriger la vulnérabilité, avertir ses clients en temps et en heure, de façon privée dans un premier temps, puis publiquement par la suite. Il y a un certain nombre de bonnes pratiques à suivre. Il est à l'avantage des autorités publiques, au niveau français ou européen, de promouvoir ces bonnes pratiques en matière de gestion des vulnérabilités.

M. Philippe Latombe, rapporteur. Vous avez évoqué dans votre propos liminaire le fait que l'on parlait beaucoup de cybersécurité pour les ordinateurs, les *datacenters*, les applications dans le *cloud*, et moins pour les téléphones mobiles, smartphones et, à terme, les objets connectés. Est-ce normal, dans le sens où nous avons déjà suffisamment à penser pour les ordinateurs, et où la réflexion sur les mobiles viendra plus tard ? De grandes entreprises ou organisations pensent-elles d'ores et déjà à la cybersécurité de leurs systèmes de télécommunications ?

M. Arnaud Dechoux. Nous assistons à un basculement très rapide des utilisations vers le mobile. Les smartphones sont aujourd'hui utilisés pour toute notre vie numérique, que ce soit pour les activités professionnelles ou personnelles. De plus en plus d'attaques visent spécifiquement les mobiles, déployées par des cybercriminels classiques ou par des États – les cyberarmes ciblant ainsi de plus en plus les mobiles.

Les enjeux sont probablement différents pour les objets connectés, qui sont produits par des entreprises qui ne sont pas spécialisées dans le numérique – qu'il s'agisse de dispositifs médicaux connectés, des imprimantes, des systèmes de ventilation, qui constituent autant de portes d'entrée pour ces cybercriminels. Beaucoup d'intrusions informatiques ont eu lieu ces dernières années à cause de portes qui n'étaient pas fermées.

Il convient pour y faire face de développer des certifications pour tous ces appareils. L'agence de l'Union européenne pour la cybersécurité (ENISA) travaille activement à l'élaboration d'un certain nombre de certifications, notamment pour les objets connectés. Cela nous semble une piste importante : il est nécessaire d'harmoniser l'approche européenne sur le sujet. L'ANSSI effectue d'excellentes qualifications et certifications, mais il est particulièrement important, surtout pour des acteurs internationaux comme nous, de mettre en œuvre une certaine harmonisation

Le deuxième enjeu est la sensibilisation. Les utilisateurs pensent encore très peu à sécuriser leurs objets connectés. De nombreuses solutions existent pourtant, notamment des solutions gratuites : nous essayons d'insister sur ce point. De très nombreux antivirus pour mobile fonctionnent très bien, détectent les mêmes attaques que sur les ordinateurs, et ont souvent des versions gratuites. De même, les gestionnaires de mots de passe changent la vie, permettent de créer des mots de passe beaucoup plus sécurisés et font gagner beaucoup de temps. Le fait de sensibiliser les entreprises et le grand public permettra d'atteindre très rapidement les objectifs, et de renforcer l'hygiène numérique au niveau national.

M. Philippe Latombe, rapporteur. Comment Kaspersky travaille-t-il avec des *start-up* ? Examinez-vous comment elles fonctionnent, pour savoir dans quelle voie il serait intéressant de travailler ? Collaborez-vous avec elles ? Les achetez-vous ? Les incubez-vous pour nouer ensuite des partenariats ? Comment rester à la pointe ? Les GAFAM achètent pour intégrer directement. Comment procédez-vous ?

M. Arnaud Dechoux. Notre *business model* est tout à fait différent. Kaspersky développe historiquement beaucoup en interne : un tiers des salariés travaille en recherche et développement. L'entreprise n'a pas l'habitude de réaliser du développement externe et d'acquérir des entreprises. Nous regardons ce qui se fait ailleurs, investissons beaucoup dans certaines technologies comme l'Intelligence artificielle (même si nous n'aimons pas le terme) et le *machine learning*, qui permet d'améliorer la détection des fichiers malveillants, en utilisant différentes techniques, notamment l'analyse comportementale. Il ne s'agit pas seulement aujourd'hui de détecter un fichier entrant, mais d'examiner des comportements inhabituels, qui peuvent générer certaines alertes. Nous investissons dans ces technologies, mais rachetons peu de sociétés.

Nous pouvons nouer des partenariats : l'un des axes importants de développement de Kaspersky est constitué des systèmes industriels, qui sont très visés. En 2019, 45 % des ordinateurs industriels protégés par les technologies Kaspersky étaient visés par des cyberattaques, qu'il s'agisse de fichiers malveillants classiques ou spécifiquement calibrés pour l'industrie. Pour développer des sondes réseau, des systèmes d'exploitation sécurisés, nous nouons des partenariats.

Kaspersky n'a pas racheté récemment d'entreprises françaises ou européennes. Tout peut changer, mais ce n'est pas la manière dont nous fonctionnons aujourd'hui.

M. Philippe Latombe, rapporteur. Excluez-vous totalement de tels rachats, ou pourraient-ils se produire à la marge si une opportunité se présentait ?

M. Arnaud Dechoux. Cela ne s'est pas fait pour l'instant, mais je ne pense pas que ce soit exclu si nous trouvons le bon partenaire pour telle utilisation particulière, ou pour faire une acquisition. L'essentiel est de trouver le bon partenariat. Nous travaillons par exemple beaucoup avec Siemens dans le domaine de la cybersécurité industrielle, les Allemands étant en pointe sur le sujet, notamment dans le secteur énergétique automobile. Nous poursuivrons ce type de démarche, sans nous interdire de faire une acquisition. Je n'ai cependant pas de scoop à ce stade.

M. Philippe Latombe, rapporteur. Je ne vous en demandais pas.

Comment voyez-vous le marché de la cybersécurité dans les deux à trois ans à venir ? Se développera-t-il fortement ? Sur quels types de technologies se développera-t-il ? À quoi sera lié le développement : les attaques extérieures qui lui feront de la publicité, la prise de conscience des directeurs des services informatiques (DSI) et responsables de la sécurité des systèmes informatiques (RSSI) ou la publicité des pouvoirs publics ?

M. Arnaud Dechoux. Les trois facteurs cités joueront. Nous nous attendons, sans surprise, à une progression stable du secteur de la cybersécurité, notamment pour les entreprises grandes et petites, en lien avec le développement des attaques elles-mêmes, de la part de groupes cybercriminels ou de groupes étatiques ou paraétatiques. Ces derniers mois, les rançongiciels ont fait l'actualité. Il n'y a aucune raison qu'ils disparaissent. Tout porte à croire que les cybercriminels continueront à mener ce genre d'attaques, d'autant que les entreprises paient fréquemment. Divers rapports parus ces derniers mois mentionnaient 30 %, 50 %, voire 70 % de paiements, ce qui alimente tout un écosystème criminel.

Des technologies de rupture sont parfois citées comme étant importantes dans le domaine de la cybersécurité. Nous pensons notamment à l'informatique quantique ; les ordinateurs quantiques parviendront-ils à casser les outils de chiffrement aujourd'hui utilisés pour protéger les données ? Beaucoup d'incertitudes demeurent sur le sujet. *A priori*, les algorithmes de chiffrement les plus avancés permettront de résister à des attaques quantiques, mais il faut continuer à investir et à utiliser dès maintenant les solutions de chiffrement les plus avancées pour prévoir cette nouvelle phase, qui peut intervenir d'ici cinq, dix ou quinze ans.

La deuxième technologie de rupture est le *machine learning*.

Pour ces différentes raisons, nous estimons que la cybersécurité continuera à progresser, peut-être davantage dans le secteur des entreprises et des organisations. Pour les particuliers, elle est de plus en plus intégrée aux outils mis à disposition par les constructeurs informatiques. Le paysage évolue beaucoup dans ce domaine, et continuera à se structurer en tout cas pour les entreprises.

M. Philippe Latombe, rapporteur. La cybersécurité des smartphones, mais aussi de l'ensemble des *devices* 5G (objets, antennes, etc.) fera-t-elle l'objet d'une attention croissante et d'un marché spécifique de la cybersécurité ?

M. Arnaud Dechoux. La réponse est ici encore clairement positive. Nos chercheurs du GReAT estiment que l'on découvrira de plus en plus de vulnérabilités dans la

technologie 5G. C'est mathématique : quand une nouvelle technologie apparaît, tout le monde en cherche les vulnérabilités, et on en trouve forcément, que ce soient des chercheurs ou les cybercriminels, qui sont sans doute ceux qui investiront le plus de temps et de moyens. En matière de 5G, ces questions de cybersécurité arriveront nécessairement dans les prochains mois, avec des attaques, des opérations d'espionnage ou de sabotage. Une vraie attention est donc requise de la part des commanditaires comme des utilisateurs, dès lors que la 5G augmentera fortement la surface d'attaque. Je n'ai pas une vision claire des dispositions de cybersécurité existantes pour la 5G, mais tout laisse à penser qu'elles seront amenées à se développer dans les prochains mois. Le phénomène est le même que pour le *cloud*, qui s'est développé de manière exponentielle ces dernières années, et a bénéficié de nouvelles technologies de cybersécurité, notamment pour le chiffrement des infrastructures. Amazon Web Services et Microsoft Azure proposent déjà une brique de chiffrement : les entreprises peuvent y ajouter une brique, pour obtenir une protection supplémentaire. Je pense que ce sera la même chose pour la 5G.

M. Philippe Latombe, rapporteur. Puisque nous parlons de *cloud*, la sécurité dans ce domaine est-elle au niveau de celle qui existe pour un serveur physique propriétaire ?

M. Arnaud Dechoux. C'est une question complexe. Tout dépend de la manière dont est protégé et configuré le serveur physique.

M. Philippe Latombe, rapporteur. On nous dit que le *Cloud Act* a invalidé le *Privacy Shield*, et que les clauses contractuelles types et les mesures de protection doivent localiser les données en Europe et les chiffrer, au repos comme en mouvement. De votre point de vue d'expert, sommes-nous en capacité de garantir (Kaspersky étant réputé pour cela) que des données au repos ou en mouvement sur le *cloud* sont chiffrées de sorte qu'elles soient quasi inaccessibles ? Ces données ne peuvent pas être considérées comme inaccessibles, par nature : mathématiquement, il existe toujours une possibilité de les déchiffrer, mais est-ce tellement compliqué que cela en devienne une vraie protection ? Est-on capable de le garantir ? C'est une des questions qui font que l'on utilise encore pour des données sensibles des *clouds* américains, en se protégeant derrière cette sorte de bouclier. Ce bouclier est-il aujourd'hui suffisant selon Kaspersky ?

M. Arnaud Dechoux. Le niveau général de protection des infrastructures du *cloud* nous paraît très bon. Pour se protéger contre des accès tiers, il faut utiliser une brique de chiffrement et de gestion d'accès tierce. Beaucoup d'acteurs français proposent ce service – Atos ou autres –, en plus du service de l'hébergeur américain ou autre. Avec ces prestataires tiers, on arrive à un excellent niveau de protection.

Au-delà de l'aspect technique, la question se pose ensuite des assurances que l'hébergeur *cloud* peut apporter que personne d'autre ne pourra avoir accès aux données, et de la manière dont il peut gérer les vulnérabilités. Ces derniers mois, des vulnérabilités ont été trouvées sur les serveurs Microsoft Exchange : cette découverte a été largement exploitée par tous types d'acteurs, *a priori*, d'autant qu'elle n'a pas pu être corrigée suffisamment tôt. Des acteurs malveillants ont pu en tirer profit. La question est celle de la manière dont ces vulnérabilités sont gérées, depuis le moment auquel les clients sont informés, pour que l'éditeur puisse *patcher* la vulnérabilité et tous les utilisateurs mettre à jour leur logiciel en temps et en heure. Dans les petites entreprises et les petites collectivités territoriales, le problème est souvent que les mises à jour ne sont pas faites rapidement, même si l'information est rapidement disponible. Le CERT de l'ANSSI est extrêmement efficace et reconnu : il publie des alertes très régulièrement. Encore faut-il que les petits acteurs en aient

connaissance et mettent à jour leurs solutions rapidement pour corriger les failles. Nous en revenons aux questions de sensibilisation et d'hygiène numérique. C'est probablement ici que le bât blesse : les mises à jour et la gestion des vulnérabilités.

M. Philippe Latombe, rapporteur. Parmi les menaces existantes, nous avons constaté l'existence d'une mode d'attaque sur les hôpitaux, pour ainsi dire. Ont-ils été attaqués en raison de la crise sanitaire, parce qu'ils possédaient des informations sensibles, ou parce qu'ils étaient faciles à attaquer ? Vous avez indiqué dans votre propos liminaire que la fréquence de circulation des virus était beaucoup plus importante aujourd'hui, d'un par jour à un par heure et un par seconde. S'agit-il d'abord d'attaques criminelles, ou d'attaques géopolitiques ? Quelles sont leurs proportions respectives ? Comment s'en prémunir en France et en Europe, en parvenant à distinguer ce qui est de nature criminelle de ce qui relève du géostratégique ?

Je prends l'exemple de l'attaque du Centre national de l'enseignement à distance (CNED) la semaine passée, attribuée aux Russes. Pourquoi effectuer une attaque en déni d'accès au service ? Quel est l'intérêt ? S'agit-il vraiment d'une attaque criminelle ? Aucune rançon n'a manifestement été demandée. À quoi servait l'attaque ?

M. Arnaud Dechoux. C'est une excellente question. Pour ce qui est des établissements de santé, les attaques s'expliquent, d'une part, parce qu'ils sont moins bien protégés, et, d'autre part, parce qu'un rançongiciel perturbe fortement leur activité, et qu'ils sont bien plus susceptibles de payer. En Allemagne, l'année dernière, on a fait état du premier décès dû à un ransomware, un hôpital touché ayant dû transporter un patient dans un autre hôpital, lequel patient est mort pendant le transfert. Je ne connais pas les détails de cette affaire, qui montre cependant bien les impacts concrets qui peuvent inciter un établissement de santé à payer une rançon plus qu'une autre victime d'attaque. Au début du confinement, l'année dernière, un collectif de hackers s'est engagé publiquement à ne pas attaquer des établissements de santé. Cela a fait long feu : les attaques ont été multipliées par quatre ou cinq pour les établissements français, selon les chiffres de l'ANSSI.

Il s'agit ici à mon sens plutôt d'attaques criminelles à visée financière. Néanmoins, vous avez raison de souligner cette question : il existe une vraie porosité entre cybercriminels et acteurs étatiques.

Ils peuvent, d'une part, se revendre des outils ou des accès sur le marché noir. On a constaté une vraie progression de ce phénomène au cours des derniers mois, sinon pour la Chine ou la Russie, du moins avec des acteurs secondaires comme l'Iran, qui avaient moins de capacités cyber, mais ont fortement progressé au cours des dernières années.

D'autre part, une attaque à visée économique peut cacher autre chose. Un service de renseignement voulant réaliser des actions d'espionnage peut compromettre certains postes et y installer des sondes ou autres, puis revendre les accès sur le marché noir à un groupe cybercriminel y déployant par la suite un ransomware. Il est parfois très compliqué de dire qui est derrière une attaque. Plusieurs acteurs peuvent être impliqués. Il s'agit d'un vrai enjeu aujourd'hui, et nous avons besoin de travailler avec les différents pays et acteurs industriels et académiques pour y répondre mieux.

Pour ce qui est des attaques du CNED, je ne suis pas dans le secret des dieux. J'ai lu dans la presse que l'attaque viendrait de Russie ou de Chine. Néanmoins, je doute que des services de renseignements ou autres groupes étatiques aient commandité ce genre d'attaque.

Un scénario que nous pouvons envisager est que des acteurs français ou étrangers aient fait appel à des *botnets*, ou réseaux d'ordinateurs zombies, envoyant beaucoup de requêtes sur le site du CNED ou d'un espace numérique de travail (ENT) pour le faire tomber. C'est déjà ce qui s'était largement produit en mars 2020, au début du premier confinement, lorsque de nombreux instituts éducatifs passaient au numérique. Nous avions déjà constaté une forte augmentation de ces attaques par déni de service, venant de réseaux d'ordinateurs situés à l'étranger. Nous voyons effectivement des adresses IP venant de l'étranger, mais je doute que ces attaques soient commanditées par un État – même si je n'ai pas d'information précise sur l'attaque du CNED de la semaine dernière. Cela illustre en tout cas encore une fois l'interaction constante entre tous ces acteurs, et le fait que ce soit une problématique mondiale.

M. Philippe Latombe, rapporteur. Avec l'incendie d'OVH à Strasbourg, nous avons constaté qu'un certain nombre d'entreprises ou d'administrations, qui lui avaient confié leurs données, avaient complètement oublié les règles de base des plans de continuité et de reprise d'activité (PCA et PRA). Lorsque Kaspersky contracte avec un client, a-t-il pour rôle de le conseiller sur ce type de sujet ? Votre objectif est d'éviter qu'un rançongiciel bloque l'entreprise cliente, mais vous ne pouvez pas tout protéger. La sensibilisation à ce sujet fait-elle partie de la prophylaxie que vous mettez en place lorsque vous contractez avec vos clients ?

M. Arnaud Dechoux. Sur le principe, cela est le cas, mais dans les faits, le rôle de Kaspersky est limité à la fourniture de solutions informatiques ainsi qu'à l'aide et au support à sa configuration et à son maintien. L'établissement de plans de résilience et de restauration est plutôt du rôle du consultant, de l'intégrateur ou du revendeur de la solution. Nous ne sommes pas toujours aux côtés du client directement : ce sont souvent des intégrateurs ou des sociétés de conseil qui assurent ce rôle. L'incendie d'OVH a effectivement très bien montré cette nécessité, qui n'est pas encore une réalité en France.

M. Philippe Latombe, rapporteur. Qui serait le bon interlocuteur pour des TPE, PME et entreprises de taille intermédiaire (ETI) sur des questions de cybersécurité ? S'agit-il de Bpifrance, lorsqu'elle finance la montée en compétences numériques des entreprises ? S'agit-il de l'intégrateur, qui est leur interlocuteur au moment de la mise en œuvre ? S'agit-il de l'expert-comptable, qui est l'interlocuteur naturel de ce type d'entreprise ? Est-ce l'assureur, qui doit augmenter ou baisser ses primes en fonction du niveau de protection ? Tout le monde doit-il prendre sa part ? Est-ce suffisant dans ce cas ? Selon vous, comment faire pour diffuser cette culture de la cybersécurité *by design*, plutôt qu'après avoir pensé le système d'information ? Quel est l'interlocuteur le plus facile pour l'entreprise ?

M. Arnaud Dechoux. Cette question est compliquée. Il peut exister plusieurs canaux. La puissance publique a sans doute un rôle à jouer dans la commande, en instaurant des seuils de budgets dédiés à la cybersécurité. C'est ce que le gouvernement a fait pour la première fois dans le volet cyber du plan de relance, qui impose aux établissements de santé de consacrer 5 % à 10 % de leur budget IT à la cybersécurité. Cela me semble une première piste.

Pour le reste, il convient de passer par les acteurs que vous avez mentionnés. J'y ajoute Cybermalveillance, né en 2017 seulement, mais qui s'est beaucoup développé depuis cette date. Il s'agit d'un réel succès, qui manque toutefois encore de notoriété. Alors que l'ANSSI se charge très bien des grands opérateurs, collectivités territoriales ou autres, Cybermalveillance doit mener les mêmes tâches pour tous les autres acteurs. Je pense qu'il faut leur donner plus de moyens et de visibilité, en réalisant des campagnes grand public.

Un autre type d'acteurs pour les collectivités territoriales est celui des opérateurs publics de services numériques (OPSN). Ils sont une cinquantaine en France, regroupés au sein de l'association Déclic. Ils aident à la mutualisation et au soutien informatique, en particulier cyber, de toutes les petites collectivités territoriales, qui sont souvent celles qui se font attaquer aujourd'hui. Il faut miser sur ces acteurs. De manière générale, la mutualisation et la régionalisation sur lesquelles le gouvernement a souhaité insister dans son plan de relance cyber me semblent de très bons axes d'action. Les OPSN sont des interlocuteurs existants sur lesquels il est pertinent de se baser, pour les collectivités locales en particulier.

M. Philippe Latombe, rapporteur. Nous en prenons bonne note. Voyez-vous un sujet que nous n'aurions pas abordé et que vous voudriez mentionner ?

M. Arnaud Dechoux. Non, c'était très complet. Nous n'avons pas parlé beaucoup du niveau européen. Je voudrais simplement souligner que la dernière stratégie européenne de cybersécurité me semble très solide. Les autorités françaises et l'ANSSI ont elles-mêmes indiqué être satisfaites de ce nouveau plan, même s'il doit sans doute être renforcé sur certains points. Pour notre part, nous insistons sur le nécessaire renforcement des dispositifs de partage d'information et de collaboration entre public et privé, qui nous semble un moyen important de progresser. En tout cas, beaucoup de choses peuvent et doivent se faire au niveau européen. Nous continuerons à suivre ces sujets.

La séance est levée à 12 heures 15.

Membres présents ou excusés

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

Réunion du mardi 13 avril à onze heures quinze

Présents. – M. Philippe Latombe, Jean-Luc Warsmann