ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Mercredi
29 septembre 2021
Séance de 16 heures

Compte rendu n° 23

SESSION EXTRAORDINAIRE DE 2021

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

ASSEMBLÉE NATIONALE

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

Mercredi 29 septembre 2021

La séance est ouverte à seize heures dix minutes.

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

———

M. le Président Alexandre Freschi. Monsieur Gérôme Billois, je vous remercie d'avoir bien voulu répondre à notre invitation. Vous êtes partenaire en cybersécurité et en confiance numérique au sein du cabinet de conseil Wavestone et membre du bureau de la commission Cybersécurité de Numeum. Je précise que Numeum est issu de la fusion, en juin dernier, de Syntec Numérique et de Tech In France, et qu'il s'agit de la principale organisation représentative des entreprises du numérique.

Vous avez également été le rapporteur général, en 2018, de l'étude de l'institut Montaigne intitulée *Cybermenace : avis de tempête* et vous publiez régulièrement des articles sur le site de cet institut.

M. Gérôme Billois, membre du bureau de la commission Cybersécurité de Numeum. Numeum est une association professionnelle qui regroupe 2 300 entreprises représentant 85 % du chiffre d'affaires du secteur du numérique en France, soit environ 60 milliards d'euros. Nous y avons une commission consacrée à la cybersécurité.

Votre mission est centrée sur des problématiques de résilience cyber. Je vais adopter à la fois une vision d'ensemble des acteurs du secteur du numérique et une approche plus concrète de praticien. En effet, dans mon activité professionnelle au sein du cabinet Wavestone, nous venons en aide aux entreprises victimes de cyberattaques en nous déplaçant sur le terrain.

La cyberrésilience est un sujet complexe. Les fragilités intrinsèques de la France et de l'ensemble des États dans ce domaine ont été démontrées. Le premier facteur expliquant la difficulté de résilience en cas d'attaque est l'uniformisation des technologies très largement utilisées dans le numérique. C'est le principal vecteur favorisant les attaques à la limite de l'ordre systémique que l'on a déjà pu observer. L'attaque NotPetya venait d'Ukraine et visait l'État ukrainien, mais l'interconnexion des différents systèmes numériques l'a amenée à toucher simultanément et très rapidement des entreprises du monde entier. Une entreprise que nous avons accompagnée a vu 50 000 de ses ordinateurs détruits en quarante-cinq minutes. La Maison-Blanche a estimé le coût de cette attaque à environ 10 milliards de dollars à l'échelle internationale. Certains grands groupes internationaux ont fait part de pertes de 600 à 700 millions de dollars, et le groupe Saint-Gobain, touché par l'attaque, a indiqué un impact de 220 millions d'euros.

Le deuxième facteur de fragilité est lié au retard dans l'investissement des entreprises, des pouvoirs publics et de l'ensemble de la sphère numérique dans la sécurisation des systèmes. Le retard accumulé dans les investissements est de l'ordre de dix à quinze ans, malgré une prise de conscience croissante. Les États-Unis, souvent cités comme leaders dans le domaine du numérique, ont fait l'objet d'attaques touchant tous les secteurs de leur

économie, comme l'essence, la distribution de viande ou les hôpitaux. Cette problématique doit être pensée à l'échelle mondiale.

Par ailleurs, il est nécessaire de mieux sécuriser par défaut tous les systèmes numériques que l'on construit. Dans les années 1970, les ceintures de sécurité étaient en option dans les voitures, seules les personnes les plus consciencieuses en demandaient l'installation. Il en va de même pour le numérique. Quand on achète un équipement numérique ou un logiciel, la sécurité n'est souvent pas implémentée par défaut… De même que le nombre de morts sur la route a amené à des obligations de sécurisation des véhicules, il faut permettre au grand public, aux TPE et aux PME d'évaluer la sécurité numérique lors de l'achat. La Commission européenne est mobilisée sur la création de mécanismes de certification, afin que le label CE puisse intégrer des éléments de cybersécurité.

Je souligne que nous sommes ici face à de vrais attaquants. Il peut s'agir d'individus isolés qui attaquent par idéologie, de groupes criminels motivés par l'appât du gain, ou d'États qui suivent une logique d'espionnage et de déstabilisation. Tous sont mus par un sentiment d'impunité. Malgré le nombre d'attaques, il existe peu de moyens pour enquêter et chercher les cybercriminels. En France la police et la gendarmerie ont fourni des efforts importants. CyberGEND centralise les forces cyber au sein de la gendarmerie, mais la justice reste le maillon faible de la chaîne : le parquet national cyber ne dispose que de trois magistrats qui doivent traiter 400 à 600 affaires par an. Les efforts doivent être menés à l'échelle française et diplomatique : la coopération internationale est nécessaire, car les cybercriminels n'attaquent que rarement leur propre pays et savent masquer leurs traces. Quelques arrestations notables ont pu avoir lieu en début d'année, grâce à des coopérations avec l'Ukraine où certains groupes criminels sont localisés.

Enfin, nous manquons de personnels et de compétences dans ce domaine. Avec l'institut Montaigne, nous avions travaillé sur un scénario d'ouragan cyber qui se déplacerait en France en emportant dans une attaque simultanée des milliers de PME, un certain nombre de grands groupes et quelques ministères. Pour gérer un tel incident et reconstruire les systèmes, nous manquerions de bras même en mobilisant les secteurs public et privé. Nous avions réfléchi à des logiques de coopération entre entreprises d'un même secteur d'activité et à l'échelle internationale, essentielles pour gérer des attaques majeures.

Toutes ces démarches sont lancées, mais nécessitent aujourd'hui d'être accélérées.

M. Thomas Gassilloud, rapporteur. Notre mission veut évaluer les grands risques pour la nation et la manière d'y faire face. En matière d'internet et de cybersécurité, on parle souvent des risques intentionnels, mais il existe aussi des risques d'incident et des risques de dépendance envers un État tiers qui pourraient nous mettre en position de fragilité. Certains grands ensembles géostratégiques comme la Chine et la Russie cherchent à s'isoler du monde cyber. Les États-Unis ne le font pas, peut-être parce qu'ils ont les clés de l'internet et se protègent ainsi. Le Royaume-Uni n'y est pas non plus poussé du fait de sa relation particulière avec les États-Unis. Mais la France et l'Europe ne se préoccupent pas de leur capacité à maîtriser leur internet. Que savez-vous de la manière de procéder de la Chine et de la Russie pour isoler leur réseau internet ? Par ailleurs, les Américains pourraient-ils couper notre internet ?

M. Gérôme Billois. Cette question n'a pas été traitée à Numeum et je m'exprime donc à titre personnel. Il faut se demander quelle est la finalité de cette isolation. Elle permet de protéger les systèmes numériques d'un pays et de limiter les influences étrangères pour

mieux maîtriser ce qui se passe dans le territoire. Technologiquement, la réalisation de l'une de ces finalités rend l'autre possible. Cela soulève le problème du respect de la liberté d'expression et de la vie privée, qui tend à s'opposer à la sécurité dans ces débats.

Techniquement, internet est un énorme nuage de réseaux assemblés les uns avec les autres. Nous pourrions cependant établir une cartographie physique de cet internet et appliquer à certains endroits des mécanismes techniques pour couper, filtrer, analyser en profondeur le réseau. Cela présente toutefois une limite technologique, car il faut des équipements puissants pour ne pas impacter la qualité du réseau. En Chine, l'accès à des systèmes en dehors du territoire national est rendu difficile par les temps de réponse requis.

M. Thomas Gassilloud, rapporteur. Il s'agit aussi d'une stratégie de la Chine pour valoriser les services numériques qu'elle héberge. Ce protectionnisme n'a rien de nouveau. Ce qui me fait peur, c'est l'absence de frontières internationales ou européennes dans ce monde de l'internet extrêmement ouvert. Quand les crises reviennent, on redécouvre l'intérêt des frontières. Cette question doit être posée pour des questions d'indépendance par rapport à des ensembles stratégiques tiers, et parce qu'internet a une telle importance dans la vie quotidienne que des accidents pourraient être dramatiques. Nous auditionnons après vous des opérateurs de câbles sous-marins, lesquels sont moins de 500 dans le monde et véhiculent 90 % du trafic international. Les marines de guerre référencent ces câbles sous-marins et nous sommes conscients de possibles stratégies de nuisance.

Comment rendre internet plus résilient à l'échelle européenne ? Un service hébergé chez un tiers et qui n'aurait pas de redondance ne serait plus accessible si les câbles transatlantiques étaient coupés, mais l'internet fonctionnerait-il toujours dans son essence même ? Nos serveurs DNS, nos règles de routages sont-ils autonomes ?

M. Gérôme Billois. Je n'ai pas les compétences techniques pour répondre de manière ferme et précise. Des acteurs comme l'AFNIC – association française pour le nommage internet en coopération –, qui gère les noms de domaines en France, ont une vision plus technique sur ces questions.

Techniquement, il est possible d'avoir une copie des services numériques essentiels en France pour que les sites en « .fr » et notre routage fonctionnent, pour des services hébergés en France et qui s'appuient sur des ressources localisées en France car certains sites en « .fr » font en réalité appel à d'autres services.

Cette stratégie nous protégerait-elle d'attaques cyber ? Il existe plusieurs types d'attaque. Les attaques par saturation consistent à envoyer plusieurs attaques depuis différents points, de façon à surcharger les serveurs en France pour les faire tomber. Si l'attaque provient de l'étranger, il suffit alors de couper les liens réseau. Mais les attaques récentes venaient de partout à la fois et il est difficile de filtrer de telles attaques. Dans le cas des attaques en temps réel, l'attaquant vise un système et en capte les données. On peut interrompre l'attaque en coupant le lien sur lequel il se trouve ou en bloquant son flux. Les attaques les plus graves, qui pourraient remettre en cause la résilience, sont celles qui s'auto-propageraient, comme NotPetya et Wannacry. Quand un attaquant cherche à faire tomber une grande partie des systèmes numériques, il ne peut pas passer d'un système à l'autre. Il crée alors une attaque qui s'autoréplique, comme un virus. À partir du moment où le virus est présent à l'intérieur du territoire, une fermeture des frontières n'est plus efficace.

Nous avions réfléchi, avec l'institut Montaigne, à la création d'un bouton rouge. Ce concept existe de plus en plus dans les grandes entreprises pour fermer tous les systèmes lorsque l'on identifie une cyberattaque en cours. C'est ce que nous mettons en œuvre avec Wavestone dans un certain nombre d'entreprises afin qu'elles puissent s'isoler en cas d'attaque. L'objectif est de limiter les impacts pour les entreprises attaquées, mais aussi de ne pas en contaminer d'autres, car de telles attaques soulèvent la question de la responsabilité des entreprises.

Mme Carole Bureau-Bonnard. Vous avez parlé de mécanismes de coopérations avec nos partenaires alliés. La multiplicité des attaques ne limite-t-elle pas la coopération par elle-même ? Dans le cas d'une attaque de la part d'un État ou sur des PME, quelles sont les solutions ? La présence dans les entreprises ou les hôpitaux de matériels étrangers ne limite-t-elle pas intrinsèquement le niveau de sécurité ? Enfin, ne faut-il pas réfléchir à des investissements pour les menaces de demain plutôt que de prendre du temps pour rattraper notre retard actuel ?

M. Gérôme Billois. La coopération n'est pas la même selon l'attaquant. Quand il s'agit d'un attaquant isolé, motivé par une idéologie, ou de groupes de criminels qui ne sont pas directement liés à des États, la coopération peut jouer pleinement. Elle manque aujourd'hui de rapidité et d'efficacité, plus à cause de la saturation des différents services que d'un manque de volonté. Les délais de réquisition criminelle entre pays sont de l'ordre de trois à six mois, alors que le cybercriminel agit en quelques jours. Les limites de la coopération apparaissent lorsque des industries sont en jeu, car on entre alors dans le champ de l'espionnage économique. Les leviers et le niveau de confiance ne sont pas les mêmes.

La même réflexion vaut pour les équipements étrangers. Nos principaux fournisseurs de solutions de cybersécurité, comme les États-Unis ou Israël, auraient peu d'intérêt à conduire les hôpitaux français à dysfonctionner. C'est en revanche différent pour les industries de défense ou de recherche et développement, pour lesquelles une réponse consiste à accumuler des produits de sécurité d'origines différentes pour lutter contre le manque de coopération de certains acteurs. Nous devons absolument conserver de la souveraineté dans ce domaine. Notre souveraineté est capitale dans le chiffrement de nos communications, afin de conserver la confidentialité de ce que nous échangeons dans les périmètres les plus sensibles ; elle l'est aussi pour la capacité de détection d'attaque. Cette dernière permet de remonter la piste d'une attaque et de mettre les attaquants devant leurs responsabilités.

S'agissant de nos retards d'investissements, les systèmes d'information fonctionnent généralement de manière itérative : une entreprise ou une administration change un ordinateur, puis une application. Les anciennes technologies sont rarement enlevées. La progression vers le haut est très lente. Les systèmes numériques des usines de distribution d'eau ou d'énergie existent parfois depuis quinze ou vingt ans et ont été pensés pour durer encore une dizaine d'années. Tout ne peut pas être changé d'un coup. Par conséquent, nous nous trouvons dans une course à la sécurisation progressive.

Mme Carole Bureau-Bonnard. Les grandes entreprises ont généralement déjà un système de sécurisation et sont conscientes du risque. L'enjeu est de sensibiliser les PME et PMI, moins organisées, pour les aider à rattraper le retard sur l'ensemble de leur défense cyber. Est-ce bien votre propos ? C'est du moins ce discours que nous devrions porter en tant que députés.

M. Gérôme Billois. Il est important de les acculturer au risque. Les PME et PMI souffrent souvent d'une pénurie de compétences pour gérer le sujet informatique. Au lieu d'un directeur des systèmes d'information, elles ont généralement quelqu'un qui fait fonctionner les ordinateurs et elles s'appuient sur un prestataire local. Il faut donc faire monter en compétence et en puissance les prestataires de services informatiques qui opèrent auprès de ces entreprises. La plateforme de l'État *cybermalveillance.gouv* référence et labellise des fournisseurs avec un niveau minimum de cybersécurité. C'est un levier très important. Par ailleurs, il faut s'assurer que toutes les offres numériques à disposition de ces entreprises intègrent par défaut une cybersécurité. C'est déjà un peu le cas, mais il faut le développer davantage.

Pour cela, il faut que les dirigeants d'entreprises qui acquièrent ces systèmes acceptent une offre un peu plus chère, dans la limite du raisonnable. Je ne parle pas d'une augmentation de 20 à 30 %. Les voitures sans ceintures de sécurité et sans airbags étaient vendues moins cher, mais aujourd'hui personne ne ferait des économies sur ces protections. Dans le numérique, les processus d'achat suivent une logique d'économies et il existe une certaine tendance à rogner sur la sécurité informatique. Les dirigeants d'entreprise doivent comprendre que cet investissement n'est pas vain, mais bien nécessaire à leur entreprise.

M. le président Alexandre Freschi. Des administrations et des hôpitaux public ont été touchés par des cyberattaques. Avez-vous le sentiment qu'il n'y a pas assez de moyens en termes de cybersécurité pour nous protéger ?

M. Gérôme Billois. Oui. Ce manque de moyens est malheureusement général. Il est même criant dans certaines entités publiques. Les hôpitaux sont dans une situation particulière, car ils ont beaucoup de systèmes fournis par d'autres et sur lesquels ils n'ont pas toujours la main. La pénurie de compétences touche encore plus le secteur public pour des questions de rémunération. La rémunération des compétences cyber augmente et constitue même une forme de bulle. La sphère publique peut avoir plus de difficultés à suivre cette augmentation que le privé.

Wavestone maintient un *benchmark* du niveau de la cybersécurité de soixante-dix grandes entreprises. La moitié d'entre elles fait partie des groupes du CAC 40. Leur niveau de conformité moyen par rapport aux référentiels internationaux de sécurité est autour de 50 %. Et tous les cybercriminels le savent ! En toute honnêteté, ce qui limite la cybercriminalité, c'est le manque de cybercriminels.

M. le président Alexandre Freschi. D'où viennent ces cybercriminels ?

M. Gérôme Billois. Parmi les trois familles que j'ai évoquées, les plus dangereux sont les groupes de criminels organisés, qu'ils soient autonomes ou liés à des mafias. Ces trois ou quatre dernières années, ils ont réussi leur transformation numérique en adoptant un mode plateforme. Avant, des cybercriminels expérimentés développaient leurs outils, attaquaient, puis récupéraient leurs gains. Aujourd'hui, ils ont créé des plateformes, comme Ryuk, REvil, Dark Side ou Conti. Ils y recrutent des affiliés, des cybercriminels débutants qui conduisent l'attaque avec les outils des plus expérimentés. Ils disposent de vrais logiciels d'attaque intégrés, avec un module d'attaque, d'exfiltration de données et de négociation de la rançon. Les affiliés récupèrent 70 % de cette dernière et la plateforme 30 %. Le quadruplement du nombre de cyberattaques par rançongiciel ces dernières années est lié à cette nouvelle échelle d'attaque, plus qu'au télétravail ou à la pandémie comme on a pu l'entendre.

La majorité de ces groupes criminels est localisée en Europe de l'Est, dans des pays russophones ou en Russie, et est organisée en équipes de dix à vingt personnes. Quelques-unes de ces sortes de PME du cybercrime ont démantelées et nous ont fourni des informations. Les États-Unis sont mobilisés sur ce sujet, qui était au cœur de la rencontre entre les présidents Joe Biden et Vladimir Poutine il y a quelques mois. En effet, même si la Russie ne mandate pas ces attaques, elle a une forme de responsabilité une fois que les groupes criminels et les individus ont été identifiés.

M. Thomas Gassilloud, rapporteur. Quelle vision avez-vous de l'articulation entre le commandement de la défense cyber, le ComCyber, et la société civile ? Historiquement, la défense protège les frontières, mais, en matière cyber, le risque peut provenir de partout. Votre rapport produit il y a quelques années formulait des préconisations sur les réservistes de la cyberdéfense et sur une fertilisation croisée entre le ministère des armées et des entreprises.

M. Gérôme Billois. Je pense à titre personnel qu'il existe une bonne articulation entre les différentes forces cyber françaises. Le périmètre du ComCyber est très clair : il traite des opérations de l'armée, de la défense des systèmes d'information de cette dernière et de sa capacité d'attaque dans le cyberespace. L'agence nationale de la sécurité des systèmes d'information, l'ANSSI, se consacre à la défense du territoire et à des fonctions critiques. Elle fonctionne main dans la main avec le ministère de l'intérieur sur les questions liées à la justice, à la police et à la gendarmerie.

Cette organisation me semble assez claire et efficace, y compris par comparaison avec d'autres pays. Sa limite est qu'elle est très tournée vers la défense du pays et manque de posture politique pour développer une économie autour de la cybersécurité. Au Royaume-Uni, le DCMS, qui équivaut à notre secrétariat d'État au numérique, porte politiquement le développement de produits et de solutions autour de la cybersécurité. Nous avons besoin de cela pour développer des structures rentables et une expertise, et financer de la recherche et du développement. La cybersécurité ne sera ainsi plus un mal nécessaire dans lequel il faut investir à finances perdues, mais un véritable axe de développement économique. En ne nous contentant pas d'acheter des équipements extérieurs, nous développerions des méthodes de protection et de défense. Cet aspect manque dans le plan annoncé par le président Emmanuel Macron dans le milieu de l'année. Malgré tout, ce plan marque pour la première fois une inflexion vers un investissement dans le développement de cette économie. Nos alliés et néanmoins concurrents, procèdent ainsi depuis plusieurs années déjà. C'est aussi un frein à la défense de notre pays.

M. Thomas Gassilloud, rapporteur. Les impacts de la crise sanitaire nous ont énormément surpris. Jusqu'où peuvent aller les impacts d'un problème majeur de cybersécurité ? Nous connaissons les armements dont disposent les États en matière cinétique et nous pouvons évaluer les dommages d'un affrontement cinétique entre deux États de même taille. En matière cyber, il est difficile d'évaluer les dégâts d'une confrontation entre plusieurs États. Êtes-vous capable d'évaluer les outils dont pourraient disposer certains États pour mener une cyberattaque massive ? Pourraient-ils paralyser un pays ?

Mme Carole Bureau-Bonnard. Quelles sont les pistes pour acculturer les générations futures à la cybersécurité dans son ensemble, afin que les jeunes deviennent des acteurs de la vie économique et sociale dans ce domaine ?

M. Gérôme Billois. Les exemples de dégâts sont parlants. À Kiev, une cyberattaque attribuée à la Russie a entraîné une coupure d'électricité pendant huit heures. L'attaque visait

les systèmes de distribution électrique et est parvenue à détruire les systèmes numériques électriques. Il a fallu redémarrer tous les postes électriques un à un. De la même façon, une attaque attribuée à l'Iran, qui a heureusement échoué, a mis en danger les systèmes de sûreté dans une raffinerie en Arabie saoudite. Ces systèmes de sûreté vérifient ce qui se passe au sein d'une raffinerie afin de tout couper en cas de risque d'explosion : cette attaque aurait pu mener à une catastrophe.

Les États s'arment dans le numérique avec des outils de recherche de vulnérabilités, de failles de sécurité, qu'on nomme dans le jargon « zeroday », car jamais un jour ne s'écoule entre le moment où on l'utilise et celui où elle est connue par l'éditeur. Ces failles sont inconnues avant l'attaque et on ne peut qu'y réagir après-coup. C'était le cas de l'affaire Pegasus, où une faille inconnue d'Apple dans les IPhone permettait d'en prendre le contrôle en envoyant un simple SMS. Dans un scénario d'attaque simultanée sur les systèmes les plus répandus tels que Windows, 50 à 60 % des systèmes numériques à l'échelle du pays seraient à l'arrêt pendant au moins trois semaines, et deux à trois mois seraient nécessaires pour s'en remettre totalement. Chez Saint-Gobain, l'activité a été interrompue pendant plus de deux semaines. Wavestone y avait pourtant envoyé une équipe de quarante personnes qui ont travaillé jour et nuit pendant trois semaines pour remettre les systèmes en état de marche, et plusieurs centaines de personnes coopéraient dans la cellule de crise. Nous pourrions également subir des attaques plus ciblées, visant des éléments clés d'infrastructure, dans les raffineries ou les centrales électriques , avec des conséquences graves dans le monde réel. Toutefois, pour généraliser ces attaques et pour faire sauter cinq raffineries simultanément ou couper l'électricité dans quinze villes à la fois, il faudrait une attaque extrêmement précise.

Qui y aurait un intérêt ? Dans la doctrine de tous les États occidentaux, chacun sait que les cyberattaques dans le monde réel peuvent entraîner une réponse appuyée sur les moyens cinétiques que vous citiez. Ainsi, si une telle attaque est techniquement possible, la probabilité qu'un État y procède est peu élevée. Le risque serait plutôt un accident : de même qu'un virus sort parfois d'un laboratoire, un outil en expérimentation pourrait se retrouver dans la nature. La probabilité qu'un tel outil soit responsable d'une attaque massive est toutefois faible.

M. Thomas Gassilloud, rapporteur. Vous vous demandez quel État aurait un intérêt à cela. Nous vivons aujourd'hui dans un monde de paix. Mais il faut imaginer que nous pourrions, demain, nous trouver en conflit ouvert avec un autre État, et que nos compétiteurs stratégiques pourraient mener des cyberattaques en parallèle d'une confrontation cinétique, en France ou ailleurs.

Vous avez évoqué les attaques qui cherchent à exploiter des failles. Peut-on imaginer que les concepteurs de systèmes laissent volontairement des portes ouvertes pour permettre aux autorités ou à eux-mêmes d'accéder au système, dans des logiciels ou même dans les équipements matériels ? Je sais que certains éditeurs laissent volontairement des portes ouvertes. Sont-elles motivées par une demande des autorités afin de prendre le contrôle des matériels à l'insu des propriétaires des équipements ? Existe-t-il un risque que ces États disposent de bombes logiques, leur permettant d'intervenir massivement sur les systèmes d'information au travers de portes dérobées non détectées ?

M. Gérôme Billois. Le risque d'une destruction des systèmes les plus critiques en France est identifié depuis la loi de programmation militaire de 2014. Nous sommes l'un des premiers États au monde à être allé aussi loin en matière de sécurisation des systèmes les plus vitaux pour la nation. Les 220 opérateurs d'importance vitale (OIV) ont tous identifié la liste

des systèmes d'importance vitale et je peux témoigner des investissements qu'ils ont réalisés pour élever le niveau de sécurité. Les États-Unis rattrapent aussi leur retard dans ce domaine. Des attaques très ciblées peuvent malgré tout survenir.

Il existe deux grandes familles de portes dérobées. Les premières existent à la suite d'erreurs, de paresse ou de facilité des développeurs. Elles ne relèvent pas d'une intention volontaire de nuire, mais représentent par la suite un véritable risque, car il s'agit de failles utilisables par tout un chacun. Les révélations d'Edward Snowden issues des renseignements américains ont prouvé par ailleurs l'existence de portes dérobées intentionnelles utilisées pour conserver un avantage stratégique. Elles sont institutionnalisées afin d'accéder à un certain nombre d'équipements, et peuvent fragiliser des mécanismes de sécurité, en particulier de chiffrement. Certains algorithmes de chiffrement comportaient des failles connues des services de renseignement pour faciliter le décryptage des données sans en posséder la clé. C'est le jeu de la cyberdéfense. Des logiciels peuvent être piégés à l'insu de leur développeur, comme dans le cas du logiciel SolarWinds : un logiciel piégé se répand et est largement utilisé, et l'attaquant peut ensuite conduire son attaque avec le plus grand effet possible. Les États cherchent à se prépositionner dans le domaine cyber, pour être en mesure d'agir le jour où ils le désireront. Des autorités, dans certains États, identifient des traces de prépositionnements d'autres États dans leurs infrastructures. C'est une pratique qui existe et qui est efficace pour les attaquants.

Madame Bureau-Bonnard, vous souligniez à juste titre que l'enjeu à moyen terme est d'aller vers la jeunesse. Il faut sensibiliser les jeunes gens au risque numérique et au principe de la vie privée sur les réseaux sociaux et sur internet, afin de les initier à la logique de la cybersécurité. La génération future devrait être sensibilisée au risque numérique comme elle l'est déjà à l'environnement. L'école a un rôle à jouer sur cette question.

Mme Carole Bureau-Bonnard. N'est-ce pas la génération actuelle, plutôt que la génération future, qu'il faut sensibiliser ?

M. Gérôme Billois. Nous avons de grandes difficultés à rendre ces actions concrètes auprès de la génération actuelle. Dans le cadre de l'association ISA-France, nous avons créé un cahier de vacances pour les 8-11 ans sur la cybersécurité, approuvé par le secrétariat d'État au numérique, ainsi qu'un jeu pour les 11-14 ans. J'ai personnellement relancé trois fois ma mairie afin que ce cahier de vacances soit distribué largement, sans réponse. Nous travaillons aussi au niveau de l'éducation nationale, et, si nous constatons quelques avancées, la prise de conscience de ce risque reste néanmoins encore lente. L'effet d'entraînement et de passage à l'échelle se fait encore attendre. C'est la raison pour laquelle je parle de génération future.

La réunion se termine à dix-sept heures et vingt minutes.

Membres présents ou excusés

Mission d'information sur la résilience nationale

Présents. - Mme Carole Bureau-Bonnard, M. Alexandre Freschi, M. Thomas Gassilloud