ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission d'enquête sur la sûreté et la sécurité des installations nucléaires

Jeudi
19 avril 2018
Séance de 10 heures 45

Compte rendu n° 28

SESSION ORDINAIRE DE **2017-2018**

Présidence de M. Paul Christophe, *Président*

ASSEMBLÉE NATIONALE

La commission d’enquête sur la sûreté et la sécurité des installations nucléaires a entendu M. Guillaume Poupard, directeur général de l’Agence nationale de sécurité des systèmes informatiques (ANSSI).

M. le président Paul Christophe. Mesdames, messieurs, chers collègues, nous accueillons maintenant M. Guillaume Poupard, directeur général de l’Agence nationale de la sécurité des systèmes d'information (ANSSI).

Créée en 2009, l’ANSSI est un service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN).

L’ANSSI est chargée à la fois d’un service de veille, de détection, d’alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État, et de la promotion des bonnes pratiques numériques auprès des administrations, des entreprises et du public.

Les effectifs de l’agence sont passés de 120 équivalents temps plein (ETP) à sa création à environ 550 aujourd’hui. Il est prévu qu’ils augmentent de 25 ETP par an jusqu’en 2022.

L’article 6 de l’ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées de déposer sous serment. Elles doivent jurer de dire la vérité, toute la vérité, rien que la vérité. Je vous invite, monsieur Poupard, à lever la main droite et à dire : « Je le jure ».

(M. Guillaume Poupard prête serment.)

M. le président Paul Christophe. Je vais maintenant vous donner la parole pour un exposé liminaire que je vous propose de limiter à une dizaine de minutes.

Je donnerai ensuite la parole à Mme la rapporteure qui vous posera un certain nombre de questions, puis les autres membres de la commission d’enquête pourront également vous interroger.

M. Guillaume Poupard, directeur général de l’Agence nationale de sécurité des systèmes informatiques (ANSSI). Monsieur le président, comme vous l’avez souligné, l’ANSSI, créée en 2009, est une agence très jeune.

Sa raison d’être est le développement de la sécurité numérique, consubstantiel au développement du numérique lui-même, lequel touche tous les secteurs d’activité, que ce soit au sein de l’État, sur le plan économique ou dans notre vie quotidienne. Dans ce cadre, le rôle de l’Agence est d’anticiper, de détecter les attaques, notamment sur le périmètre ministériel et administratif, voire au-delà demain. Ce sujet fait l’objet d’un texte porté dans le cadre de la loi de programmation militaire qui adresse des propositions à l’ANSSI.

L’ANSSI est également capable de réagir, en ce qu’elle est en mesure d’aider les victimes en cas d’attaques. C’est ainsi que des « pompiers numériques » aident les victimes, sans en faire état. En effet, lorsque nous sommes confrontés à des attaques à des fins de vols d’informations, la plupart du temps, les victimes ne veulent pas que cela se sache afin d’éviter tout sur-accident immédiat. Au-delà de l’impact direct de la perte d’information, c’est la confiance de leurs partenaires et de leurs clients qui est susceptible d’être entachée.

Il n’en reste pas moins que des attaques sont visibles. Il s’agit pour l’essentiel d’attaques à des fins de sabotage. La France a eu à connaître le cas un peu emblématique de TV 5 en 2015, que nous avons utilisé pour faire de la sensibilisation. TV 5, qui n’était pas une entité très robuste en termes de sécurité numérique, a été agressée par un attaquant extrêmement efficace qui a cherché à détruire l’ensemble du système de production de TV 5. Par chance, nous sommes intervenus très rapidement et la chaîne a fort bien réagi.

Plus récemment, au printemps dernier, l’ANSSI a connu une activité extrêmement chargée dans la mesure où elle a été confrontée concomitamment à plusieurs scénarios qu’elle avait anticipés. Cela dit, anticiper ne suffit pas toujours. Nous avons été confrontés à une campagne d’attaques criminelles « Wannacry » à des fins d’extorsion d’argent. C’est ainsi que les virus prennent le contrôle de réseaux informatiques, chiffrent les données et proposent aux victimes de retrouver l’accès à leurs données en échange d’une rançon. Le système de rançon de Wannacry fonctionnait très mal, au point que les personnes qui souhaitaient payer ne récupéraient pas leurs données pour autant.

Au surplus, la dissémination a été extrêmement violente et rapide, elle n’était absolument pas ciblée. Heureusement, la France n’a connu que très peu de victimes, mais il y en a eu d’assez emblématiques de par le monde. Je pense notamment aux services de santé britanniques qui ont été extrêmement perturbés. Pendant plusieurs jours, ils ont été dans l’impossibilité d’aiguiller les malades et les ambulances vers tel ou tel hôpital. Nous avons des difficultés à mesurer les conséquences liées aux problématiques de sécurité numérique au sens de vols d’informations, qui soulèvent la question de la sécurité des personnes.

Nous avons dû faire face à une seconde vague d’attaques au printemps dernier qui répondaient au nom de Notpetya, à des fins de destruction pure et simple, menées dans le cadre de conflits, déclarés ou non. Il a été avéré que l’Ukraine était ciblée. La France a connu des victimes parce que les ramifications des réseaux numériques de certains utilisateurs s’étendent jusqu’en Ukraine. C’est ainsi que la société Saint-Gobain a été touchée. Les conséquences pour la société n’ont pas été anodines puisque l’informatique de Saint-Gobain a été paralysée pendant quinze jours. Au-delà de l’impact sur l’image, l’impact économique se répercute sur les comptes de l’entreprise. Saint-Gobain évoque une perte nette de 80 millions d’euros. Ce qui, très cyniquement, m’intéresse en termes de sensibilisation car, au-delà des autres problèmes posés, un tel exemple souligne l’impact économique réel de la cybersécurité.

Ce n’est pas anecdotique : de nouvelles menaces se développent, notamment contre nos démocraties. Nous avons été très occupés l’an dernier par la sécurité des élections présidentielles et législatives afin d’éviter toute forme d’ingérence informatique dans les systèmes de l’État. On peut tout imaginer, qu’il s’agisse du risque de modification des résultats, de la problématique du vote des Français de l’étranger qui a été laissée de côté faute de maturité à ce moment-là, des attaques possibles contre les partis politiques et des équipes de campagne – qui sont un problème nouveau et intéressant pour nous. Plus personne aujourd’hui ne peut s’estimer à l’abri des risques numériques.

Nous disposons de plusieurs leviers d’action. Tout d’abord, un levier réglementaire. La France a été le premier pays au monde, ce dont nous sommes très fiers, à affirmer que ces sujets sont trop graves pour se limiter à des actions de sensibilisation et de conseil. Des articles très importants sur la cybersécurité sont portés par la loi de programmation militaire votée en décembre 2013. Ils imposent aux opérateurs critiques de mettre en place des règles de cybersécurité dans différents secteurs d’importance vitale. Le nucléaire civil fait partie de ces secteurs et les règles de sécurité figurent sous forme d’arrêtés sectoriels. Publiques, d’un

niveau assez générique, ces règles imposent aux opérateurs eux-mêmes, en lien avec le ministère coordonnateur, des actions à mener en termes de gouvernance, d'organisation, de mise en place de moyens techniques sur les systèmes dits d'importance vitale, c'est-à-dire les systèmes les plus critiques, par ces opérateurs d'importance vitale. L'idée n'est pas de faire de la réglementation pour le plaisir, mais de trouver les moyens efficaces pour élever le niveau de sécurité des opérateurs critiques. À cet égard, l'ANSSI contrôle l'action des opérateurs par la voie d'un canal privilégié. Ces derniers sont obligés de notifier à l'ANSSI les incidents liés à la sécurité, ce qui lui permet de s'assurer que leur volonté n'est pas de cacher la poussière sous le tapis. L'idée est d'être capable de les aider au plus vite en cas de problèmes et surtout d'avoir l'information pour s'assurer que le même type de problème ne se produit pas chez d'autres acteurs.

Par expérience, nous savons que les cyber-attaquants se focalisent rarement sur une cible unique, mais se spécialisent plutôt dans divers domaines d'activité, que ce soit à des fins d'espionnage économique ou à des fins de caractère plus militaire. Dans le cas du nucléaire, les scénarios que nous anticipons mettent en jeu des acteurs susceptibles de s'intéresser à l'ensemble du sujet sur les différents types d'opérateurs pour toucher les points les plus fragiles. Une cohérence défensive est à mettre en place. Nous utilisons la réglementation pour agir.

Récemment, nous avons transposé la directive européenne sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS », *Network and Information Security*, qui reprend, à l'échelle européenne, les idées que nous avions développées parallèlement en France et en Allemagne. Suite à la loi de transposition qui a été votée à la fin de février 2018, nous pouvons dorénavant appliquer la même logique aux opérateurs de services essentiels. L'idée consiste à identifier des acteurs critiques, d'en identifier progressivement de plus en plus et de mener cette démarche réglementaire. Comme toute forme de réglementation, cette réglementation est bienveillante et se présente comme une main tendue en vue de catalyser le développement de la sécurité numérique chez ces opérateurs qui, pour beaucoup d'entre eux, découvrent le numérique et, bien davantage encore, la sécurité numérique. Le sujet concerne tout le monde, y compris ceux qui ne sont pas experts dans le domaine de la cybersécurité.

Nous voulons faire remonter ces sujets au plus haut niveau de la gouvernance parce que les impacts sont majeurs en termes de fonctionnement, d'arbitrages financiers et de conception même des systèmes. On ne fait pas de la cybersécurité en passant le bon contrat avec une entreprise ou bien en embauchant trois experts : l'activité est plus diluée, elle est transverse au fonctionnement de l'ensemble des acteurs. C'est à la fois tout l'intérêt et toute la difficulté qui s'attache à cette problématique.

Le cas des centrales nucléaires est un peu particulier. Je tiens en général un discours assez anxiogène et assez critique car je suis très inquiet de ce que l'on relève dans différents secteurs. Nous ne sommes pas prêts à résister à une cyber-attaque massive. Je pense que nous avons fait beaucoup mais le champ est si vaste et nécessite tant d'évolutions de process que si un grand État voulait porter atteinte aujourd'hui à notre sécurité numérique, les conséquences, malheureusement, seraient assez graves.

Le cas du nucléaire est un peu particulier. Le sujet est emblématique quand on parle de sécurité en général. Dès 2012, avec l'aide du ministère en charge de l'énergie, l'ANSSI s'est rapprochée d'EDF pour mettre en avant la question que posaient les centrales et la nécessité de la traiter. Notre démarche avec EDF a été originale, car elle a été exhaustive et

s’est traduite par une suite d’audits. L’ANSSI s’est rendue sur place pour étudier le niveau de sécurité réel, et pas uniquement théorique, de l’ensemble des centrales nucléaires du parc français.

Ces audits sont coopératifs. Nos auditeurs ont les capacités et le savoir-faire des attaquants informatiques. Pour gagner du temps, en coopération avec EDF, nous leur donnons accès à une large documentation relative aux centrales et à des plateformes afin qu’ils gagnent du temps. Le but des attaquants est de trouver toutes les failles possibles, de pénétrer au sein des systèmes et de mesurer les effets qu’ils peuvent obtenir. Il s’agit d’attaques réalisées dans des conditions maîtrisées. Nous procédons ainsi régulièrement dans les ministères et chez de multiples opérateurs d’importance vitale. Nous réalisons à peu près soixante-dix audits par an, ce qui est considérable en termes d’activité.

À chaque fois, nous fixons des règles du jeu à nos attaquants : ils ne doivent rien casser et rester responsables mais sont libres de leurs attaques. L’idée est de les positionner en tant que véritables attaquants qui voudraient porter atteinte à la sécurité des systèmes. En termes d’effets à obtenir, nous nous attachons aux atteintes à la sécurité des centrales et à leur sûreté de fonctionnement, à la possibilité de voler de l’information sensible, de bloquer la production d’électricité sans pour autant détruire. Les attaquants ont le droit de passer par le réseau, par les clés USB, par les réseaux sans fil, par les ondes ou par des réseaux non physiques.

À l’issue de ces audits, qui incluent également une étude de l’organisation car nous avons une approche théorique parallèle, nous sommes amenés à formuler des recommandations. Il nous arrive d’identifier des vulnérabilités réelles. Dans le cas des centrales, c’est assez rare et c’est pourquoi je le mentionne, rien de grave n’a été trouvé. Nous pouvons toutefois être amenés à faire des recommandations de défense en profondeur. Parfois, on pose plusieurs barrières. Quand bien même la première barrière n’a pu être franchie, il n’en reste pas moins que, tel le château fort, édifier plusieurs barrières permet de s’assurer que si un attaquant réussissait à passer une première étape, il resterait bloqué ensuite.

À partir de 2012, nous avons adressé des recommandations à EDF dans un process d’amélioration continue. Nous réalisons des audits très poussés et formulons des recommandations qui sont prises en compte. Je reconnais que nos remarques sont intégrées et impliquent parfois des modifications du système. Lorsque de nouveaux paliers ou que des évolutions de versions interviennent, nous procédons à de nouvelles évaluations. Nous effectuons en moyenne tous les ans un ou deux audits des centrales.

Mme Barbara Pompili, rapporteure. Dans chaque centrale ?

M. Guillaume Poupard. Non, nous étudions des centrales représentatives. Lorsqu’elles sont identiques d’un point de vue numérique, nous réalisons un seul audit. Un ou deux créneaux sont préréservés par an. Bien entendu, nous portons une attention toute particulière aux systèmes les plus modernes en nous étant assurés que les systèmes anciens n’étaient pas vulnérables. Bien entendu, plus il y aura de numérique, plus le potentiel de vulnérabilité sera grand, plus il faudra être vigilant. Bien évidemment, nous regardons l’EPR avec beaucoup d’attention. L’avantage, c’est que nous avons pu étudier très tôt sa conception numérique. Dès 2012, nous avons été en lien étroit avec EDF. Le sens de l’histoire veut que les centrales, comme tout système industriel, s’engagent de plus en plus sur la voie du numérique. L’ambition vise à s’assurer que ce numérique supplémentaire, qui certes viendra

enrichir l'existant, n'affaiblira pas les nouveaux systèmes. Portée par la réglementation, c'est l'action que nous menons de manière itérative et incrémentale. Cela dit, EDF s'était engagée sur cette voie volontairement avant même la mise en place de la réglementation.

M. le président Paul Christophe. Monsieur Poupard, merci de ces propos introductifs.

Madame la rapporteure, je vous cède la parole.

Mme Barbara Pompili, rapporteure. Monsieur Poupard, nous vous avons adressé un questionnaire auquel nous vous serons reconnaissants de répondre précisément.

Vous dites gérer globalement la question de la sécurité informatique en France. Avez-vous estimé les moyens alloués au nucléaire ?

M. Guillaume Poupard. À l'exception de Thomas Hautesserres, qui est coordonnateur et qui s'assure de la bonne relation entre les opérateurs externes à l'ANSSI et l'interne, les agents ne sont pas spécialisés par secteur d'activité. Nous avons des experts par métier, des personnes qui sont capables de faire de l'audit, de l'accompagnement dans la conception de systèmes, de la certification, mais personne, au sein de l'ANSSI, n'est affecté uniquement au nucléaire.

Nous pourrions mesurer la charge que représente le nucléaire en ETP. Un audit requiert la présence de 6 à 8 personnes pendant trois mois, ce qui est peu et beaucoup. Cela nous permet un niveau de visibilité précis des vulnérabilités éventuelles. Presque toujours, les agents trouvent des failles, parfois graves dans certains domaines autres que le nucléaire. J'insiste sur ce point, car c'est l'un des rares cas où les réunions de restitution d'audit ne sont pas des drames antiques, précisément parce que les agents ne trouvent pas grand-chose. Des mesures, qui ne sont pas des mesures de sécurité numérique, mais d'architecture, de séparation de certains composants, avec le contrôle-commande d'un côté, les questions de sûreté de l'autre, aident à introduire de la sécurité, rendant le système plus difficile à attaquer, un peu à l'instar du secteur aérien. Lorsque des acteurs sont très sensibilisés aux questions de sécurité par nature, même s'il ne s'agit pas de sécurité numérique à l'origine, il est plus facile de travailler avec eux. Il en va de même des banques. Je cite les cas positifs. Malheureusement, des cas sont beaucoup plus négatifs. Je pense aux organismes qui estiment qu'il n'y a pas de risques et dont le niveau de sécurité est très souvent extrêmement faible.

Si je vous dis que l'ANSSI emploie en moyenne entre 5 et 10 ETP pour traiter du nucléaire, je ne dois pas être loin du compte.

Mme Barbara Pompili, rapporteure. Estimez-vous qu'un ou deux audits par an sur les installations nucléaires sont suffisants au regard de la rapidité avec laquelle évoluent les techniques ? Les citoyens que nous sommes entendons que les *hackers* ont toujours une longueur d'avance.

M. Guillaume Poupard. C'est vrai, nous courons après les *hackers*, des attaquants extrêmement agiles. Les centrales n'évoluent pas d'un palier par jour. Le gros problème réside dans les secteurs numériques qui, aujourd'hui, évoluent à toute allure, notamment le numérique grand public. Ma tablette se met à jour constamment, je ne sais plus ce qu'elle fait. Ce serait très difficile à auditer. Il en va différemment des centrales qui évoluent par palier très précis, cadencé, les paliers sont espacés par un temps. Le travail que nous avons

accumulé depuis 2012 nous a permis de rattraper la dette en termes d'audit. Nous pouvons ainsi nous intéresser à chaque nouveau palier qui se présente. Concrètement, pour répondre à votre question, j'ai l'impression que nous avons cette idée de versionnage très précis. Nous validons une version globalement, nous la mettons en place, la nouvelle version intervient assez longtemps après. Aujourd'hui, si je plaçais deux fois plus d'agents sur la sécurité nucléaire civile, je ne suis pas certain que nous ferions davantage. Notre visibilité est exhaustive. Je le dis car c'est probablement le seul cas où nous avons une visibilité aussi exhaustive de la situation. Habituellement, l'idée même des inspections et des contrôles c'est de faire de l'échantillonnage. Nous avons pu aller au-delà de l'échantillonnage parce que c'est possible et parce que nous avons commencé depuis assez longtemps déjà.

Mme Barbara Pompili, rapporteure. Au cours de votre travail, avez-vous été informé de plans de cyberattaques contre des centrales nucléaires françaises ?

M. Guillaume Poupard. Non, pas contre des centrales ou des installations. Je suis extrêmement prudent. Le sujet est très actuel. Depuis plusieurs mois, nous observons des activités inquiétantes sur des secteurs d'importance vitale, notamment de l'énergie. Il ne s'agit pas d'attaques à proprement parler mais c'est encore plus angoissant, car nous observons des attaquants qui cherchent à entrer au sein de réseaux, qui ne volent ni ne cassent rien pour l'instant ; ils sont manifestement en train de préparer des coups futurs. Nos alliés britanniques, américains et allemands observent le même phénomène. Les attaquants sont les mêmes. Les Anglo-Saxons attribuent ces actes ; les Français, pour l'heure, ne le font pas. Déterminer qui se cache derrière une attaque est très compliqué. Nous restons extrêmement prudents, nous ne voulons pas tomber dans des pièges ni nous tromper dans l'attribution des attaques qui, pour l'heure, ne présentent aucun effet repéré.

Le secteur le plus sensible – plus par une analyse des faits – est le secteur de l'énergie. Perdre l'énergie serait catastrophique pour l'ensemble des activités. Ce n'est pas tant de ne plus avoir de centrales nucléaires qui serait problématique, c'est l'ensemble de la chaîne qui serait mis en cause. C'est la raison pour laquelle nous travaillons sur les centrales, mais à l'autre bout de la chaîne, nous travaillons aussi beaucoup avec Linky de façon à sécuriser les compteurs intelligents. Un compteur intelligent qui est attaqué, même s'il s'agit d'un fait négatif, reste un fait divers ; en revanche, si tous les compteurs d'une ville se faisaient attaquer en même temps, nous serions confrontés à un effet systémique nouveau qui serait dramatique. Si nous voulons obtenir des effets, ce n'est pas forcément la source, mais l'ensemble des maillons de la chaîne énergétique qu'il nous faut sécuriser. L'attaquant lancera son offensive au point le plus facile. Aujourd'hui, nous avons la conviction que le plus facile n'est pas d'attaquer les centrales car ce sont les installations les plus protégées. À cet égard, nous n'avons rien observé de concret, nous n'avons constaté aucune trace d'attaques informatiques qui auraient fonctionné contre des centrales françaises. En revanche, au sein de réseaux de télécommunication, nous relevons des traces d'activité anormale d'attaquants de haut niveau qui préparent de mauvais coups. Peut-être même ne savent-ils pas eux-mêmes encore ce qu'ils préparent. Récemment, j'ai employé une image un peu triviale et anxiogène. Il faut s'imaginer des armées étrangères qui viendraient placer des charges explosives sous le Pont de l'Alma pour le cas où, un jour, leurs autorités leur demanderaient de faire sauter le pont. Malheureusement, dans le cas du numérique, c'est un peu ce qui est en train de se produire. Des conflits futurs se préparent dans le numérique, c'est très inquiétant, mais pas contre les centrales nucléaires.

Mme Barbara Pompili, rapporteure. On nous a souvent dit au cours de nos auditions que les réseaux internet des centrales seraient étanches aux cyberattaques. Que

signifie « étanches » ? Si elles le sont, comment cela se matérialise-t-il ? Nous avons largement évoqué les ports USB. La présence de ports USB rend l'étanchéité relative. Vous êtes-vous penché sur ces questions ?

M. Guillaume Poupard. C'est ce à quoi nous nous attachons en priorité. J'espère ne contredire personne – ou tant pis si c'est le cas ! –, mais les réseaux étanches, au sens de réseaux informatiques qui n'auraient aucune communication à aucun moment avec l'extérieur, quelle que soit la définition que l'on retient du terme « extérieur », n'existent pas. Les réseaux totalement autistes, sauf cas très exceptionnels, n'existent pas. Dans tous les secteurs, le propre d'un réseau informatique est d'être en mesure de faire du pilotage, de remonter et de recevoir certaines données. Même s'il ne s'agit pas de fonctionnement courant et quotidien du réseau, quand des mises à jour d'équipements, de logiciels, une connexion au réseau se réalisent, l'étanchéité n'est pas parfaite. Y compris sur le plan de la conception, on a renoncé à cette idée, faite pour se rassurer, de systèmes totalement autonomes et fermés vis-à-vis de connexions informatiques, d'internet ou de clés USB. Parmi les nombreux systèmes que nous avons étudiés, les plus anciens n'avaient pas de port USB, mais ils avaient des lecteurs de disquettes. Ce sont des portes d'entrée et de sortie. La notion d'étanchéité est assez conceptuelle ; en tout cas, dans la réalité, l'étanchéité n'est jamais parfaite. C'est évidemment aux points de vulnérabilité que nous nous attachons.

Ce que je puis dire de la conception des centrales – et c'est ce que me disent mes experts –, deux points restent totalement séparés : le système de contrôle-commande et les mécanismes de sûreté. Les systèmes de contrôle-commande sont les systèmes numériques qui permettent de commander le fonctionnement de la centrale. L'on a d'un côté les systèmes qui font fonctionner la centrale, de l'autre, les mécanismes de sûreté qui, s'ils détectent un fonctionnement anormal dans l'activité de la centrale, enclenchent des processus de sécurité. Dans leur conception même, ces deux fonctions, dans les centrales, sont séparées. C'est extrêmement rassurant.

En cas d'accès au système de contrôle-commande, des données pourraient être prélevées qui remonteraient et qui, probablement, sortiraient des systèmes. De telles voies existent. Au cours des audits, nous nous attachons très précisément à la manière dont on peut entrer ou sortir d'un système depuis internet. Ce sont les menaces les plus graves, mais il ne faut pas oublier qu'une personne à l'intérieur de la centrale pourrait également intervenir. Je connais peu d'endroits où l'on puisse s'assurer que personne ne trahira jamais, volontairement ou non. Ce peut être un ingénieur comme du personnel de ménage. On peut tout imaginer et il convient d'anticiper.

Dans le cadre des audits, nous prenons en compte les scénarios où une personne ayant accès à une machine branchera une clé USB sans même savoir ce qu'elle fait. Il est possible qu'on lui ait demandé de connecter telle clé sur telle machine, sans rien faire d'autre. Le scénario est anticipé et des mécanismes de protection mis en place, que nous sommes amenés à expertiser et que nous préconisons de durcir. Un gros travail a été entrepris par EDF pour que ces liens ne soient pas de la connexion informatique. Ce sont des systèmes de diodes, par exemple, pour s'assurer que les données ne peuvent aller que dans un sens. On parle aussi de découplage protocolaire, de systèmes conçus sur mesure. Ce n'est même plus de l'informatique, mais de l'électronique, seule passe l'information qui doit passer. Un virus, par exemple, ne peut passer par ce biais.

Lorsque les clés USB ou de telles connexions sont nécessaires, nous mettons en place des batteries de mesures qui n'autorisent que les seules clés identifiées. Nous utilisons

des mécanismes cryptographiques pour éviter qu'une clé venant de l'extérieur puisse être branchée et pour la rendre inactive. Dans certains cas, les ports USB ont été retirés pour supprimer toute connexion physique. Ces éléments sont de nature à rassurer. Une fois encore, je ne peux assurer qu'il n'y a aucune entrée/sortie, mais ces entrées/sorties sont les points les plus étudiés dans le cadre des audits, voire dès la conception des systèmes car ce sont les points de fragilité.

S'agissant des points plus aisés d'accès, tels que les réseaux sans fil, wifi entre autres, nous y portons une attention particulière. Pour un attaquant, l'accès est facilité. Mais l'hypothèse d'un attaquant qui pourrait accéder à des prises physiques sans passer par des réseaux sans fil est également prise en compte, *a fortiori* dans le cas de réseaux sans fil. Ces points font l'objet de toute notre vigilance. Si cela était mal fait, nous serions confrontés à des vulnérabilités béantes mais tel n'est pas le cas à l'heure actuelle, car nous avons porté tous nos efforts sur ce point.

Mme Barbara Pompili, rapporteure. Autrement dit, même s'il y a du wifi, tout va bien ? Je pose la question, car je me suis retrouvée dans la salle des commandes de l'EPR de Flamanville où il y avait du wifi. Comme je le faisais remarquer aux responsables présents, il m'a été répondu que l'EPR n'était pas en fonctionnement. J'ai objecté la présence d'informations dans les ordinateurs.

M. Guillaume Poupard. Il faut évidemment vérifier attentivement que le wifi ne permet pas de se connecter à des réseaux sensibles. Quand bien même n'y aurait-il pas de wifi, d'autres systèmes existent comme la 3G et la 4G qui permettent de capter des données. J'ignore ce qui est précisément fait à ce titre. Mais si du wifi connecté permettait aux smartphones – encore que je ne sois pas certain que l'utilisation des smartphones soit autorisée n'importe où dans une centrale – de surfer sur internet, pour autant, ce n'est pas la centrale qui est concernée.

Ces sujets sont donc étudiés en premier. Certains de nos experts sont dédiés uniquement aux technologies sans fil, sujet qui nous intéressent depuis l'origine, car il s'agit d'une source de vulnérabilité supplémentaire si les réseaux sont mal conçus.

À cette thématique « radio », deux menaces sont liées : d'une part, des réseaux utilisent des techniques radio pour se connecter ; d'autre part, il existe un risque d'agressions électromagnétiques. Les ondes électromagnétiques sont une menace que nous connaissons depuis longtemps et qui sont susceptibles de détruire des équipements. Le cas extrême est celui de la bombe nucléaire qui explose en altitude et qui produit ce que l'on appelle des impulsions électromagnétiques. Nous savons nous en protéger. C'est ainsi que les équipements qui doivent être absolument inattaquables et protégés de la destruction – nous sortons des cyberattaques pour nous placer sur un champ d'ordre militaire – sont protégés des ondes extérieures par des cages de Faraday, afin d'éviter une agression électromagnétique qui viserait à détruire les composants électroniques. Des protections sont prévues dans le cadre des centrales, mais elles sont réservées aux équipements qui sont essentiels, notamment aux équipements de sûreté.

Mme Barbara Pompili, rapporteure. Lorsque l'on évoque des attaques par les ondes, on pense aussi aux drones qui ont survolé plusieurs de nos centrales. De ce point de vue, cela pose le problème des informations qui pourraient être captées, ne serait-ce que des images. Avez-vous mis en place des mesures de protection contre les survols de drones ?

M. Guillaume Poupard. Cette problématique est plus du ressort du SGDSN que du mien. Je n’empiéterai donc pas sur son domaine.

S’agissant des drones, nous connaissons des cas, en sources ouvertes, où des personnes ont utilisé des drones pour se rapprocher de sources wifi et se connecter à des réseaux wifi. De toute façon, nous faisons l’hypothèse que les attaquants ont accès au réseau, même s’il est physique. Non, la problématique des drones porte davantage sur l’imagerie ou les explosifs, comme nous le voyons sur des terrains de guerre, en Syrie notamment. Ce n’est pas notre problématique. Quant aux techniques contre les drones – hypertechnologie de brouillage, par exemple –, l’ANSSI vient en soutien technique quand il y a besoin d’expertise, mais ce n’est pas dans notre cœur de métier. Pour la cybersécurité, la question des drones ne change pas la donne. Je ne dis pas qu’il n’y a pas de risques liés aux drones, mais sur notre sujet particulier, cela ne change rien.

Mme Barbara Pompili, rapporteure. Vous n’avez pas repéré d’attaques malveillantes à l’encontre des centrales, dites-vous. Or, quand nous avons interrogé le PDG d’Orano, il nous a dit que le groupe connaissait des attaques quotidiennes et nombreuses, une dizaine, voire une centaine d’attaques – les mêmes que celles que nous subissons tous. En revanche, il a ajouté que le groupe faisait l’objet d’une ou de deux attaques quotidiennes ciblées et délibérées.

M. Guillaume Poupard. Je ne dis pas qu'il n'y ait pas d'attaques ni d'agents menaçants, bien au contraire. L'ANSSI retient l'hypothèse que le monde est hostile, et je pense qu'il l'est, et même de plus en plus.

La question est celle du sens que l’on donne à l'expression « attaque informatique ». Mardi dernier, nous avons publié notre rapport d'activité. À cette occasion, les journalistes nous ont interrogés sur le nombre d’attaques en 2017. C’est la question que la presse nous pose systématiquement. Je suis extrêmement gêné pour répondre. Je peux dire qu'en 2017, l'ANSSI a connu vingt crises, c'est-à-dire vingt attaques majeures ; en d'autres termes, vingt attaques qui réussissent et dont les conséquences sont inacceptables pour la défense et la sécurité nationale. Douze opérations, qui ont été déclenchées par l'ANSSI, nous ont occupés plusieurs mois. Ces données ne concernent pas le nucléaire, et pas les centrales, en tout cas pas en 2017.

Par contre, d'une façon constante, des gens cherchent à entrer dans des réseaux informatiques à partir d'internet. Si vous branchez une machine sur Internet avec un logiciel pour suivre son activité, il y a immédiatement des personnes qui cherchent à se connecter. C'est automatique, ce sont d'ailleurs des robots qui sont à l'œuvre. Le temps d'infection d'une machine branchée sur internet qui n'a pas été mise à jour depuis un certain temps est de quelques minutes. C'est automatique. Je vous conseille d'ailleurs de mettre à jour votre téléphone constamment, c'est vraiment la meilleure manière de vous protéger. Une bonne partie des mises à jour est dédiée à la sécurité. C'est essentiel.

Parmi les attaques qui réussissent, on note qu'un réseau connecté à internet, ce qui n’est pas le cas des réseaux au sein des centrales, présente une opportunité pour un attaquant générique, un criminel ou un attaquant qui cible ses actions. Protéger à coup sûr un réseau connecté à internet de l'intrusion d’attaquants de haut niveau est très difficile. Nous partons donc du principe qu'un réseau connecté à internet résistera à des menaces courantes, à des virus génériques, mais ne résistera pas à des attaquants de haut niveau.

Si, un jour, on découvre que les réseaux et les équipements sensibles des centrales nucléaires sont connectés à internet, il faudra s'inquiéter car nous n'avons pas toujours la technologie appropriée pour nous protéger contre une telle faille. En revanche, nous mettons en place des logiques d'architecture pour isoler progressivement les réseaux les plus sensibles et éviter toute connexion directe à internet, par une box notamment. Ce sont là des choses bien connues qui font partie des règles que nous imposons à l'ensemble des opérateurs à l'importance vitale. Il est hors de question que les systèmes critiques soient directement connectés à internet.

Certaines attaques, de sites internet par exemple, sont traumatisantes, qui se traduisent par des dénis de service, des blocages de sites, de la défiguration. De tels cas donnent l'impression que l'attaquant a pris le contrôle de sa victime. En pratique, quand les choses sont bien faites, les sites internet ne sont pas dans le cœur du réseau informatique de l'entreprise. Ils sont ailleurs. De telles défigurations sont très désagréables et entrent dans la catégorie des attaques informatiques, mais ce n'est pas parce que le site internet a été attaqué que le réseau de l'entreprise a été atteint. Pour autant, cela entraîne très souvent une confusion. Tous les types d'attaques, tous les types d'attaquants sont confondus. Pourtant, même si cela entre sous le seul vocable de cyberattaque, la différence est grande entre un service offensif qui dispose d'énormes moyens et un petit attaquant, entre un site internet et le cœur d'une centrale. Pour toutes ces raisons, nous sommes gênés pour communiquer sur le nombre d'attaques.

Très concrètement, nous n'avons pas connaissance en France d'attaques contre les centrales nucléaires et nous n'avons pas de détection d'attaques qui auraient franchi des barrières sensibles.

Mme Barbara Pompili, rapporteure. Nous pourrions nous demander si, pour des installations aussi délicates, il ne faudrait pas couper tout apport numérique et revenir aux systèmes qui fonctionnaient sur les anciennes centrales.

M. Guillaume Poupard. Notre rôle consiste à accompagner l'évolution numérique. Je viens du secteur de l'armement. Il m'arrive de dire aux marins que, du temps de la marine à voile, il n'y avait pas de problèmes cyber, si ce n'est qu'avec des bateaux à voile on ne fait plus la guerre aujourd'hui. Le numérique fait l'efficacité des moyens modernes. La moitié de la valeur embarquée dans un bateau de guerre moderne est composée de logiciels ! Demain, ce sera 80 %. Telle est l'évolution des choses.

Dire aux acteurs de ne pas développer le numérique en raison de sa dangerosité, c'est l'assurance qu'un jour ils disparaîtront faute d'être restés compétitifs. En revanche, il faut être prudents et ne pas se précipiter vers le numérique. Certains opérateurs mettent leurs données dans le *cloud,* externalisent et connectent des tablettes non sécurisées à tout ! Certains font n'importe quoi. Le risque est alors majeur. Notre message est le suivant : il faut accompagner la transition numérique, mais cela représente un coût alors que le numérique est présenté comme un gain. La sécurité est onéreuse. Aujourd'hui, on considère que pour une activité un peu sensible, le coût de la sécurité numérique – entre l'humain, les logiciels, le matériel, etc. – représente entre 5 % et 10 % du budget informatique, soit des sommes considérables. Cela pèse souvent sur les budgets de structures auxquelles on demande par ailleurs de réaliser des économies. Les équations financières sont compliquées. Dans les cas les plus critiques, les domaines des transports, des télécoms, de l'industrie, l'évolution numérique doit être pensée en termes de sécurité et telle est la révolution qui est en train de se produire. Notre rôle est d'inciter, voire d'obliger à prendre en compte la sécurité numérique en même temps que le

numérique se développe. Il faut s'autoriser des cas où le numérique n'est pas forcément nécessaire. Je recommande aux membres du Gouvernement l'usage de téléphones sécurisés pour les questions sensibles, de téléphones fixes sécurisés pour les questions plus sensibles encore, et de s'abstenir de téléphoner pour les sujets les plus sensibles ; et encore faut-il, dans ce dernier cas, discuter dans des pièces dont on s'est assuré qu'elles sont dépourvues de micros.

Il faut apprendre à vivre avec le numérique, le dompter et utiliser les bons moyens au bon moment. Avec les centrales, le cadre reste maîtrisé. Le scénario catastrophe aurait été de passer à de nouvelles générations technologiques très technophiles avec des réseaux IP partout, élevant le risque numérique dans des proportions fortes. Le constat que je fais est que les risques ont été pris à temps et sont maîtrisés aujourd'hui, ce qui ne supprime ni le risque ni les attaquants. Des attaquants, j'ai la certitude qu'il y en aura.

Mme Barbara Pompili, rapporteure. Nous avons auditionné un parlementaire belge ; il nous a indiqué que des plans de centrales nucléaires belges circulaient sur le *dark net*. Il ne savait pas ce qu'il en était concernant les centrales nucléaires françaises. Avez-vous des informations à ce sujet ?

M. Guillaume Poupard. Je ne dispose pas d'informations particulières. J'ai vu ce qui circulait dans la presse. Je suis incapable d'infirmer ou de confirmer les propos entendus.

Les plans, qu'ils soient physiques ou de réseaux informatiques, sont une difficulté. Nous avons observé en France, pour des secteurs sensibles autres que les centrales, que des plans circulaient sur le *dark net*, voire sur internet, suite à des erreurs commises par certains. Par exemple, dans le cadre d'appel d'offres en génie civil, en réseau informatique ou en sécurité, des acteurs annexent le plan au cahier des clauses techniques particulières pour que les entreprises qui répondent à l'appel d'offres dimensionnent leur devis. On est parfois confrontés à une certaine naïveté de la part de certains acteurs ; dans d'autres cas, on souffre d'un manque de responsabilités de sous-traitants qui disposent des plans. Ils ne comprennent pas que les documents sont sensibles et les mettent en ligne sur leur serveur. Des erreurs se produisent donc, nous commençons à en faire la chasse, notamment en formant des agents qui préparent les marchés.

J'ai à l'esprit le cas étonnant d'une présentation qui avait été faite par un dirigeant de société à l'occasion d'une visite scolaire. Pour illustrer le fait qu'il existait un réseau informatique dans son entreprise, il avait ajouté à sa présentation le plan informatique exact, avec toutes les adresses IP, de son entreprise. On trouve parfois sur internet des informations qui font bondir et qui, de fait, ne sont pas classifiées alors qu'elles le mériteraient. Par le biais de marchés, de rapports avec les sous-traitants, des informations sont rendues publiques.

Je n'ai pas l'exemple de plans de centrales nucléaires françaises qui circuleraient sur le net, les donneurs d'ordre sont sensibilisés ; cela n'en reste pas moins un sujet de préoccupation. Il faut qu'un système soit bien pensé de bout en bout et éviter que l'information sensible fuite par inadvertance, méconnaissance ou pour toute autre raison, mais dont les conséquences peuvent être graves. Des plans physiques ou informatiques ne font qu'aider l'attaquant.

Les travaux que nous avons conduits avec EDF reposent sur des hypothèses extrêmement fortes. Comme nous le disons, nous n'agissons pas sur la sécurité par l'obscurité ; nous partons du principe que l'attaquant dispose de la connaissance des réseaux et

que, malgré cet avantage, il ne doit pas être en mesure d'attaquer. Pour autant, ce n'est pas une raison pour que ces plans « fuitent. »

Mme Bérengère Abba. Monsieur Poupard, vous êtes le directeur général de l'Agence nationale de la sécurité et des systèmes d'information et je vous remercie de toutes les informations d'ordre général que nous venons d'entendre.

Nous sommes confrontés à deux options.

Aujourd'hui, vous nous dites sous serment que vous estimez que tout est sous contrôle et que vous faites confiance aux systèmes de sécurité. Nous savons les risques encourus, il ne s'agit pas là d'un risque industriel banal, nous savons les conséquences que pourrait engendrer un incident ou un accident nucléaire. Si cela devait se produire, la population se retournerait vers nous.

Soit, à l'inverse, vous reconnaissez certaines vulnérabilités, certaines failles potentielles, auquel cas je doute fort que vous nous expliquiez le détail de ces risques et failles en commission publique, d'où ma question : estimez-vous utile que nous nous revoyions à huis clos ?

M. Guillaume Poupard. Vous l'avez rappelé, madame, je m'exprime sous serment. Le secteur nucléaire civil est le plus sûr, le plus mature que je connaisse parmi les secteurs sensibles que j'observe. Le secteur nucléaire est celui où le plus de travaux sont entrepris, où les obligations de moyens sont maximales. Nous ne sommes pas loin d'une obligation de résultat à la hauteur des enjeux.

Je n'affirmerai pas que le risque est partout à zéro, que tout a été vu. Je vous révélerai à huis clos les risques résiduels que nous anticipons. Quel que soit le système, de toute manière, la sécurité absolue n'existe pas. Et cela reste vrai, y compris dans d'autres systèmes qui sont presque plus sensibles que le nucléaire civil. Il faut vraiment identifier les risques résiduels et réfléchir aux mesures organisationnelles ou de contrôle qui permettent de les maîtriser. Je sais qu'une séance est prévue à huis clos avec la Secrétaire générale de la sécurité et de la défense nationale, au cours de laquelle nous pourrons aborder ces risques résiduels si vous le souhaitez. En toute honnêteté et bonne conscience, on peut dire que le risque est aujourd'hui maîtrisé. La représentation parlementaire et la population ne doivent pas éprouver de craintes.

M. Jean-Marc Zulesi. Certains sites nucléaires sensibles ne sont pas systématiquement floutés sur les images satellites de type *Google Earth*. Quel regard portez-vous sur cet aspect et comment pourrions-nous faire pour qu'elles soient floutées dans un futur proche ?

M. Guillaume Poupard. Ce sujet ne relève pas de la compétence de l'ANSSI et ma réponse vient de ce que j'entends en réunion au SGDSN. L'ANSSI, de toute façon, fait l'hypothèse que l'attaquant dispose de toutes ces informations et d'autres, bien plus précises encore. Cela fait donc partie de nos hypothèses de travail et si, un jour, l'on découvrait des plans assez détaillés, cela n'aurait aucun impact sur nos analyses de sécurité qui prennent déjà ce scénario en compte.

D'après notre expérience, la pression mise par le SGDSN et le ministère de la transition écologique et solidaire sur les opérateurs pour flouter des zones est

systématiquement payant. Toutes nos demandes sont prises en compte. Pour autant, il faut être prudent et inscrire nos efforts dans la durée, car nous savons que les bases de données sont mises à jour régulièrement et que de nouvelles photos sont prises. Nous devons nous assurer que, dans la durée, des opérateurs, tels que *Google Earth*, continuent à flouter les zones. Je n'ai pas connaissance que des opérateurs numériques aient refusé de répondre à ce genre de requêtes.

M. Anthony Cellier. J'ai bien noté votre formule « rien de grave n'est identifié » comme étant la synthèse des phases de tests que vous opériez. C'est rassurant.

Les différentes auditions que nous avons organisées sur la thématique de la cybersécurité ont fait ressortir deux arguments. D'une part, nous avons découvert que l'aspect hermétique des centrales nucléaires n'était pas absolu. D'autre part, l'ancienneté de notre parc nucléaire, qui est donc peu informatisé, présente un atout en matière de cybersécurité. Mais j'imagine que ce ne sera plus le cas des futures installations du type EPR. J'aimerais vous entendre sur ce point et sur la façon dont vous travaillez en amont sur une telle thématique.

Si l'attaque du virus Stuxnet a qui a eu lieu en 2010 avait été orientée contre nos centrales ou nos capacités de production, à cette époque-là, aurions-nous été vulnérables ?

M. Guillaume Poupard. En qualité d'ingénieur, je me dois de vous dire que les systèmes ne sont pas hermétiques à 100 %. Les moyens de communication sont extrêmement limités. La seule règle de séparation hermétique réside entre les moyens de sûreté et les moyens de contrôle des commandes du cœur.

Vous avez entièrement raison, les anciennes centrales sont protégées par leur obsolescence numérique. C'est ce que l'on rencontre dans de nombreux secteurs. Les très vieux systèmes ne sont pas attaquables, car ils sont encore électromécaniques, il n'y a pas d'informatique au sens moderne du terme. Pour les systèmes du futur, tel l'EPR, il faut impérativement prendre en compte la sécurité numérique en amont, dès la conception des systèmes, pour concevoir les architectures en pensant à la sécurité numérique dès l'origine et dans le temps.

Je parle d'une façon générique ; nous sommes plus inquiets pour les systèmes modernes qui n'ont pas été conçus en prenant en compte la sécurité numérique. De tels systèmes qui comportent beaucoup d'informatique et qui ne sont pas encore protégés sont une aubaine pour les attaquants. De ce point de vue, nous serons confrontés à des difficultés à l'avenir.

Dans le cas du nucléaire, la question de l'EPR a été identifiée dès l'origine. Nous n'avons pensé qu'à cela, l'ANSSI n'est pas seule dans ce cas, EDF en avait eu l'idée. Le travail que nous avons mené conjointement avec elle s'est avéré extrêmement positif. C'est un projet qui s'est inscrit au bon moment. Je place l'EPR dans la catégorie des systèmes futurs qui ont été « cybersécurisés » par conception. C'est plutôt très rassurant. Entre les deux zones de risque, on trouve des paliers de centrales existantes. Certains systèmes de contrôle-commande de centrales ont été numérisés. C'est ce que nous avons vérifié dans le cadre des audits ; nous sommes plutôt sereins.

Les améliorations légères que nous avons souhaitées sur des zones qui ne font pas l'objet d'attaques directes et au titre desquelles nous voulions encore progresser en sérénité ont été prises en compte par EDF dans les centrales en exploitation.

Stuxnet date de 2010. Nous avons commencé à réaliser des audits à EDF en 2012, les deux questions ne sont pas totalement décorrélées. Nous nous sommes dit qu'il ne faudrait pas que de telles attaques aient lieu en France sur des centrales nucléaires. Stuxnet est passé à l'attaque en Iran. Il s'agissait probablement d'une très grosse opération de contre-prolifération pour empêcher le développement du nucléaire militaire iranien. Personne n'a avoué en être l'auteur, mais certains arborent un grand sourire quand on en parle, ce qui n'est pas loin d'être un aveu.

Des centrifugeuses qui enrichissent du combustible à des fins militaires et qui sont des machines mécaniques contrôlées par l'informatique ont été attaquées de manière informatique. Pendant trois ans – je ne cite en l'occurrence que des sources ouvertes –, les centrifugeuses ont connu des pannes et des casses. Si l'on prend le contrôle à distance d'une centrifugeuse, qu'on l'accélère et on la freine suffisamment de fois, elle finit par casser. Ce qui est assez incroyable dans le cas de Stuxnet, c'est que les centrifugeuses en question étaient totalement déconnectées d'internet. Mais des clés USB circulaient des centrifugeuses à des systèmes plus classiques connectés à des messageries et donc à internet. Autrement dit, il est raisonnable de penser que les attaquants, par une suite de virus, dont Stuxnet, ont réussi, grâce à des clés USB, à prendre la main sur les systèmes de contrôle-commande, ces automates industriels qui gèrent les centrifugeuses.

L'opération était très discrète et pendant trois ans s'est révélée très efficace ; toutefois, à un moment donné, le virus s'est « échappé ». C'est ainsi que nous l'avons retrouvé dans de nombreux pays où il n'a rien cassé, car il était conçu pour cibler des sites précis. Cela dit, il a joué le rôle de révélateur ; nous avons réalisé que les systèmes industriels que nous anticipions comme des cibles futures étaient déjà des cibles pour les attaquants, probablement les plus compétents au monde. Nous en avons déduit que si ces derniers savaient attaquer aujourd'hui, d'autres sauraient le faire demain. En 2010, Stuxnet a réorienté une part élevée de notre politique vis-à-vis des secteurs d'importance vitale. Une attaque de type Stuxnet est le scénario typique que nous voulons empêcher et que nous prenons en compte dans le cadre de nos audits.

Mme Perrine Goulet. Nous avons beaucoup parlé des centrales nucléaires EDF. J'aimerais savoir si la sécurité est la même sur les autres sites qui détiennent des matériaux nucléaires par les autres opérateurs.

M. Guillaume Poupard. Je le pense. Nous n'exerçons toutefois pas le même degré de surveillance. Le fait de procéder à des audits systématiques et exhaustifs est unique. Il n'y a pas d'autres secteurs où ce soit le cas. Pour les systèmes les plus sensibles, les règles s'appliquent, en particulier aux opérateurs d'importance vitale. Évidemment, les conseils, recommandations et obligations s'adressent à tout le monde ; cela dit, les audits ne sont pas systématiques et je ne peux prétendre que nous ayons vérifié la totalité des systèmes, tout simplement parce que nous n'en avons pas la capacité.

M. Jimmy Pahun. Qui sont les attaquants de Stuxnet, « ceux qui sourient » ?

M. Guillaume Poupard. « Ceux qui sourient » sont des acteurs qui avaient intérêt à freiner le programme nucléaire iranien. Il s'agit de services de grands pays. C'est un cas un peu particulier car, habituellement, les attaques informatiques ne me font pas sourire. En l'occurrence, c'est un des rares cas où la finalité me paraît honorable.

M. le président Paul Christophe. Vous arrive-t-il de vous défier entre autorités ? Vous arrive-t-il de tester les réseaux des autres partenaires pour coconstruire des parades entre alliés ?

M. Guillaume Poupard. Nous n'avons pas d'amis dans le cyber-espace, nous avons d'ailleurs la preuve que nos alliés nous attaquent. Certes, le challenge mutuel existe, mais il est opérationnel, il n'est pas à blanc. Dans bien des domaines de la sécurité, la coopération peut être franche et simple, notamment dans l'antiterrorisme pour ne citer qu'un secteur, car on se doute bien que ce ne sont pas nos grands alliés qui mèneront des attaques terroristes en France. Dans le cadre de la cybersécurité, nous sommes beaucoup plus prudents. Ce n'est pas de la paranoïa ; diverses révélations, notamment dans le cadre de l'affaire Snowden, ne font que confirmer la pertinence de principes que nous appliquions d'ores et déjà à l'époque.

Les audits traitent de sujets qui relèvent de la souveraineté nationale. Nous avons de nombreux liens avec nos partenaires allemands et britanniques et un grand nombre d'échanges opérationnels, mais ils ne nous permettent pas d'auditer des infrastructures critiques entre États membres, dans la mesure où des secrets industriels doivent être protégés. Agir différemment supposerait une confiance absolue, qui serait un peu naïve si l'on tient compte des questions de sécurité économique. Nous échangeons sur les principes généraux et les méthodes d'audit mais, de là à auditer des sujets critiques chez nos partenaires, nous n'y sommes pas prêts. En revanche, nous travaillons sur des objets communs. Je pense aux avions construits en Europe et pour lesquels nous avons tout intérêt à auditer ensemble. Il en va de même pour un tunnel transfrontalier qui, par définition, est une infrastructure partagée. Mais pour les infrastructures nationales, la logique veut que nous restions à l'intérieur de nos frontières. D'ailleurs, dans l'esprit de la directive européenne NIS, nous avons rappelé aux opérateurs que chacun était responsable de ses infrastructures critiques. Aucune « infra » n'est ouverte aux 28 États membres, car cela poserait bien des problèmes.

M. Jean-Marc Zulesi. Le cyber-espace évolue en fonction des technologies et oblige de rester à la pointe des évolutions technologiques et des innovations. Je sais que vous avez un service de veille. Comment l'ANSSI reste-t-elle à la pointe de l'innovation, de la technologie et des nouvelles connaissances ?

M. Guillaume Poupard. L'ANSSI comporte une sous-direction d'environ 160 personnes, incluant des laboratoires de recherche qui, pour la moitié de leur temps, font de la recherche académique. Ce sont des laboratoires très ouverts vers l'extérieur. L'autre moitié du temps, ils entreprennent des recherches secrètes et très classifiées car on se trouve sur des cas d'attaques. Le rôle des laboratoires est d'être dans l'anticipation et dans la maîtrise des techniques de sécurité numérique. Il faut distinguer les technologies de leurs usages.

Nous n'allons pas nous mettre à courir derrière toutes les applications numériques, cela n'aurait aucun sens. En revanche, il existe toujours des invariants et notre mission consiste à anticiper les évolutions des usages à quatre ou cinq ans. Parmi les grandes évolutions passées, nous avons connu le *cloud computing*, le fait que l'informatique soit massivement sous-traitée et se retrouve dans des lieux très difficiles à identifier.

Désormais, la question de l'internet des objets ou des objets connectés transformera les champs économiques et de la vie privée. Tout se connecte et tout devient intelligent, c'est-à-dire doté de capacité de calcul et de communication. Face à de telles évolutions, l'idée consiste à mettre en place des approches et des règles pour sécuriser ces systèmes qui font évoluer les écosystèmes. Notamment dans l'industrie moderne, on trouve un ordinateur au

cm^2 ; tous les ordinateurs sont connectés sans fil. Quand deux automates doivent être connectés, plutôt que de tirer un câble de 10 centimètres, on les fait communiquer par radio. Ce sont ces techniques que nous suivons.

Nous parlons beaucoup avec les équipementiers qui sont à la source et qui ont été infectés par Stuxnet, afin que le développement numérique s'opère de manière maîtrisée. Dans les cas les plus sensibles, nous nous adressons directement aux développeurs. C'est le cas pour les centrales. Nous pouvons décider, par exemple, que telle technologie n'est pas prête, faute d'être sécurisée, et qu'il n'est donc pas possible de l'intégrer. Dans d'autres secteurs, où la pression de compétitivité est plus forte, nous recherchons toujours un bon équilibre entre la sécurité et le fait pour les entreprises de ne pas prendre de retard. Des sujets extrêmement complexes font actuellement leur apparition. Le véhicule autonome, par exemple, est un sujet majeur en termes de sécurité et pourtant tout le monde est obligé d'aller assez vite, car celui qui, dans dix ans, ne proposera pas de véhicules autonomes sera probablement voué à disparaître, y compris les grands équipementiers.

Telles sont les évolutions que nous essayons de suivre. Nous parvenons à une vision générique suffisante pour couvrir le risque, même si évidemment elle n'est pas exhaustive. Nous procédons beaucoup par recherche de coopérations.

M. Anthony Cellier. J'aimerais parler des messageries électroniques. Dans le cadre de déplacements de déchets, une organisation est mise en place. Sans doute des échanges se font-ils par emails pour expliquer les modalités du transport, le trajet qu'il suivra, à quel moment il interviendra, ce qui peut être un point de faille. Comment intervenez-vous sur l'échange par messagerie ? Y a-t-il une approche moins technique et plus comportementale vis-à-vis des usagers pour leur expliquer le bon comportement à adopter ?

M. Guillaume Poupard. Nous connaissons les solutions. Je suis incapable de vous dire si elles sont systématiquement appliquées chaque fois que nécessaire. Notre approche, qui est un peu maximaliste, consiste à dire que toute information envoyée en clair via internet ou sur un réseau téléphonique peut être potentiellement écoutée et traitée par un service de renseignement, même s'il n'est pas le service le plus puissant de la planète. Nous faisons l'hypothèse que toute information envoyée est compromise. Il n'y a donc pas 36 000 manières de se protéger. Chercher à se noyer dans le trafic est inutile dans la mesure où les services sont très doués pour trouver, parmi des masses de données, la bonne information au bon endroit. Il faut donc chiffrer l'information. Le chiffrement est une technologie majeure qui n'est pas nouvelle – on chiffre depuis 2 000 ans. Aujourd'hui, protéger l'information lors de la transmission nécessite de la chiffrer. L'ANSSI dispose des moyens de chiffrement. Elle évalue et qualifie des produits de messagerie qui permettent de procéder ainsi. Je parle de façon générique – je ne suis pas capable de vous répondre sur le cas du transport des matières dangereuses – mais je relève que, trop souvent, des gens continuent à envoyer en clair pour, ensuite, s'étonner que l'information soit connue d'autres personnes.

Le chiffrement est un outil essentiel. Pour autant, le message n'est pas facile à porter car il se présente, en apparence, en contradiction avec la problématique des services de police qui, lors des enquêtes, sont confrontés au chiffrement et au fait que les ennemis de la France ne sont pas les derniers à utiliser le chiffrement pour se protéger. Nous sommes confrontés à un paradoxe que nous ne savons pas résoudre et qui voudrait que les « gentils » utilisent le chiffrement et que les « méchants » ne l'utilisent pas. La mission de l'ANSSI étant la prévention et la protection, nous sommes très favorables au chiffrement ; nous disposons d'ailleurs de l'un des meilleurs laboratoires de cryptographie en France et au monde. Selon

nous, cette technologie est clé. Il faut seulement s'assurer de son utilisation systématique dans le cadre d'échanges sensibles, ce qui n'est pas toujours le cas.

Nous pouvons chiffrer lorsque les messageries sont gérées. Malheureusement, des échanges d'informations plus ou moins sensibles se font par des messageries instantanées de type *Whatsapp* ou *Telegram*, dont je doute qu'elles soient sécurisées ; il est très probable que des personnes sachent traiter ces messageries. Dans la mesure où on ne peut pas compter sur le fait de se cacher dans la masse, il s'agit de points de vulnérabilité. Lorsqu'ils utilisent ces outils, je mets en garde les décideurs publics et privés à ne pas envoyer d'informations sensibles susceptibles d'être traitées par des attaquants.

M. Anthony Cellier. Vous préconisez d'utiliser le cryptage pour des échanges sensibles dans le domaine du nucléaire. Mais, aujourd'hui, de ce que je peux comprendre, vous ne pouvez pas imposer à EDF de demander à son personnel d'utiliser le cryptage pour ses propres échanges sensibles.

M. Guillaume Poupard. Je pense que les ordinateurs portables sensibles sont chiffrés aujourd'hui. On ne peut compter sur le fait qu'il n'y aura ni perte ni vol – et des vols, il y en a beaucoup, c'est classique. Les technologies du chiffrement sont donc indispensables et, à ma connaissance, sont mises en place.

Mme Barbara Pompili, rapporteure. Chez les sous-traitants ?

M. Guillaume Poupard. Cela fait partie des hypothèses que nous étudions. Dans nos hypothèses, nous incluons les sous-traitants et le contexte amont. Cela n'aurait aucun sens de chercher à protéger EDF sans s'intéresser à son écosystème.

L'ensemble des sous-traitants d'EDF utilisent-ils la messagerie chiffrée pour tous leurs messages ? Je suis persuadé que ce n'est pas le cas. Mais toutes les données ne sont pas sensibles non plus. Il faut s'assurer que les éléments sensibles sont bien protégés par des technologies robustes.

M. Thomas Hautesserres, **coordinateur en charge du secteur nucléaire à l'ANSSI**. L'organisation de transports de matières nucléaires est classifiée. Dans ce cas-là, une obligation réglementaire est faite d'utiliser des technologies de chiffrement ou de ne pas passer par des réseaux à certains niveaux de sensibilité. Pour le cas des transports nucléaires, il existe une obligation réglementaire de chiffrer les informations quand elles sont relatives à des transports qui doivent être protégés.

Mme Barbara Pompili, rapporteure. Vous avez dit que les opérateurs étaient obligés de notifier les incidents de sécurité. Incluiez-vous les opérateurs nucléaires ? Comment contrôlez-vous le respect de ces obligations ?

M. Guillaume Poupard. D'abord, la loi s'applique, qui prévoit des contrôles que nous sommes amenés à effectuer et des peines pour ceux qui ne l'appliqueraient pas. C'est un ensemble assez classique de normes. Voilà pour l'aspect un peu contraint. En pratique, une fois que les opérateurs ont compris notre rôle, qu'ils ont compris que l'ANSSI est capable de garder le secret et que la notification de tels problèmes ne provoquera pas d'autres difficultés, notamment médiatiques en cascade, la confiance s'établit très rapidement. Nous nous fondons sur la recherche de partenariats de confiance qui s'appuient sur la réglementation.

Je ne peux exclure le scénario d’une collusion de l’ensemble des acteurs concernés travaillant pour un même opérateur à taire des informations à l'ANSSI mais, en pratique, je ne pense pas que cela se produise et si cela devait se produire, les conséquences seraient très graves. Autant nous sommes là pour aider les opérateurs, autant nous serons sans pitié avec ceux qui ne jouent pas le jeu. Je le leur dis d’ailleurs.

Mme Barbara Pompili, rapporteure. J'imagine bien, mais je pose la question car nous avons vu le problème se poser s’agissant de questions de sûreté très graves. Je pense au chantier de l'EPR de Flamanville. Des intérêts économiques très lourds rendent tout retard du chantier extrêmement problématique et garder le silence évite de nouveaux retards. Établir des liens de confiance est une bonne optique, mais avoir des moyens de contrôle est également important. Vous n’avez pas détaillé les moyens de contrôle.

M. Guillaume Poupard. La loi prévoit que l’ANSSI dispose de moyens de contrôle, qu’elle se rende chez les opérateurs ; nous le faisons déjà dans le cadre du nucléaire civil. Cela reste des audits, ce ne sont pas des descentes de police ou des perquisitions. Nous procédons sur un mode très coopératif. Ainsi que je vous l’ai dit, je ne peux pas exclure un scénario catastrophe où tous les efforts seraient faits pour nous cacher la copie. D'ailleurs, tel n'est pas l'état d'esprit de la loi. Il est hors de question que je place des agents de l'ANSSI en interne et en permanence pour m’assurer que l'on ne nous cache rien. Et quand bien même le ferions-nous, on pourrait imaginer des risques résiduels où les agents de l'ANSSI seraient eux-mêmes contrôlés par l'opérateur. Ici encore, il ne peut y avoir de certitudes. Telle est la raison pour laquelle je favorise cette relation de confiance qui me semble la solution la plus efficace pour obtenir une information complète. Cette relation de confiance passe, en partie, par le secret et par la préservation des intérêts des opérateurs.

M. le président Paul Christophe. Il me reste à vous remercier, monsieur Poupard. Nous nous retrouverons d’ici peu dans un autre contexte. En tout cas, merci pour la précision de vos réponses.

—⟡—⟡—

Membres présents ou excusés

Commission d’enquête sur la sûreté et la sécurité des installations nucléaires

Réunion du jeudi 19 avril 2018 à 10 h 45 :

Présents. – Mme Bérangère Abba, M. Xavier Batut, M. Anthony Cellier, M. Paul Christophe, M. Grégory Galbadon, Mme Perrine Goulet, M. Jimmy Pahun, Mme Barbara Pompili, M. Jean-Pierre Pont, M. Jean-Marc Zulesi.

Excusés. – M. Julien Aubert, Mme Émilie Cariou, M. Patrice Perrot, Mme Isabelle Rauch.