ASSEMBLÉE NATIONALE

XIII^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mercredi
1er juin 2011
Séance de 10 heures

Compte rendu n° 41

SESSION ORDINAIRE DE **2010-2011**

Présidence de M. Guy Teissier, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures.

M. le président Guy Teissier. Nous avons le plaisir d'accueillir aujourd'hui M. Patrick Pailloux, directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI) créée le 7 juillet 2009.

L'activité de votre agence est au cœur du continuum sécurité défense. La protection des systèmes informatiques constitue un enjeu essentiel dans tous les domaines, qu'il s'agisse de la défense du territoire et de nos forces ou encore de la sécurité de nos intérêts économiques.

La menace est réelle et difficilement saisissable car elle repose sur des moyens publics et privés souvent entremêlés. C'est ainsi que la presse a fait état ces derniers mois d'attaques « pirates » contre certains de nos ministères, sans que l'on soit parvenu à en établir clairement l'origine.

La maîtrise des communications peut être considérée comme une arme, d'autant plus dangereuse qu'elle est peu coûteuse et disséminée. Comme l'a révélé l'attaque informatique contre le programme nucléaire iranien, avec le fameux virus Stuxnet, son recours caractérisera très certainement nombre de conflits modernes.

Dans ce contexte, votre mission est essentiellement défensive : nous devons disposer des moyens suffisants pour prévenir et contrer toute tentative d'intrusion dans nos réseaux. Nous aimerions donc savoir si la France et notamment votre agence disposent des moyens suffisants pour protéger nos intérêts. Le Premier ministre a annoncé le 25 mai dernier un ensemble de mesures destinées à lutter contre cette menace : pourriez-vous nous en indiquer les grandes orientations ?

Vous pourrez également nous donner votre sentiment sur le degré de sensibilisation de nos responsables politiques, administratifs ou encore économiques sur ces questions. Un travail de pédagogie doit-il être envisagé ?

M. Patrick Pailloux, directeur général de l'agence nationale de la sécurité des systèmes d'information. Permettez-moi d'abord de vous remercier de me donner l'opportunité d'intervenir devant vous.

Nous vivons à l'heure des cybermenaces et il est difficile d'être optimiste sur leur évolution. Depuis quelques années les attaques informatiques à des fins crapuleuses se multiplient. Ces attaques sont essentiellement de deux ordres : le vol d'informations sensibles et le sabotage.

Depuis 2005, le nombre d'attaques ciblant délibérément des institutions et des entreprises à des fins de vol d'informations sensibles est en très forte augmentation dans le monde.

Trois motivations sont principalement à l'origine de ces agressions qui peuvent viser les pouvoirs publics comme les entreprises.

La plus traditionnelle est l'appât du gain illicite permis par la revente d'informations personnelles. La dernière affaire importante et médiatisée concerne le vol de 100 millions

d’identités, y compris des numéros de carte bancaire, chez Sony et plus précisément au sein du système gérant la console de jeu Playstation III. Dans ce genre d’affaires, les bénéfices pour les attaquants peuvent s’élever à plusieurs millions d’euros.

La seconde motivation, que l’on rencontre trop souvent et dont ne voyons au mieux que la face émergée, est l’espionnage visant à s’emparer d’informations secrètes. Dans cette catégorie, les services de l’État ont traité ces derniers mois plusieurs attaques informatiques majeures visant des grandes entreprises ainsi que celle ayant touché le ministère de l’Économie et des finances.

Enfin la motivation la plus récente, rencontrée de plus en plus fréquemment, est d’ordre politique ou idéologique. Elle vise notamment à rendre publiques des informations embarrassantes volées dans les systèmes d’information d’organismes visés. L’affaire « Wikileaks », qui n’est pas une attaque informatique, de la publication sur Internet de télégrammes diplomatiques américains, est emblématique de ce nouveau type de menaces. La France n’est naturellement pas à l’abri de telles attaques qui peuvent être dévastatrices pour l’image d’une l’institution et de ses dirigeants.

J’en viens maintenant au sabotage. On observe depuis de nombreuses années des défigurations de sites Internet ou des attaques visant à bloquer les sites pendant quelques heures ou quelques jours. En 2010, 7 000 sites répertoriés en « .fr » ont ainsi été touchés.

Dans le même ordre d’idée, le « piégeage » de matériels de télécommunication installés sur les réseaux de communications électroniques a déjà été observé, permettant au « piégeur » d’intercepter les communications.

Beaucoup plus grave, il est possible de prendre le contrôle de systèmes industriels – vannes de distribution, systèmes de production d’énergie, appareillages médicaux, – afin de les perturber voire de les détruire. L’été dernier, l’affaire dite du « ver Stuxnet » a ainsi démontré pour la première fois la faisabilité d’une attaque informatique délibérée et ciblée d’un processus industriel critique, en l’occurrence et potentiellement le programme nucléaire iranien. Si nous savions que des attaques informatiques pouvaient affecter le fonctionnement de matériels techniques tels que des équipements médicaux, il est désormais avéré qu’il est possible de porter atteinte à une infrastructure vitale par une attaque à distance de ses systèmes d’information et de contrôle.

Les agressions les plus graves peuvent avoir une finalité stratégique : comme l’ont montré les incidents en Estonie, en Géorgie ou en Iran, chaque tension politique, chaque conflit entre États, est désormais accompagné d’attaques informatiques. Récemment, une attaque apparemment menée par la Corée du Nord contre la deuxième banque de Corée du Sud a été rendue publique: les pirates ont pénétré le réseau de la banque et effacé un grand nombre de données. Il en est résulté deux semaines d’indisponibilité, l’impossibilité de verser les salaires ou encore de retirer de l’argent.

En revanche, il n’a pas encore été observé d’action terroriste contre ou à travers les réseaux même s’ils les utilisent pour leurs communications et leur propagande.

Pour répondre à cette menace, le Livre blanc sur la défense et la sécurité nationale a retenu que notre pays devait se doter d’une capacité de défense informatique. Il a recommandé que soit créée une agence nationale de la sécurité des systèmes d’information.

Cette agence a été créée le 7 juillet 2009 dernier par un décret du Premier ministre à la suite d'une mission de préfiguration mise en place dès le 1er janvier 2009.

L'ANSSI, dès sa création, s'est vu confier deux missions : une mission opérationnelle et une mission préventive.

La mission opérationnelle vise à doter la France d'une capacité de réaction en cas d'attaque informatique contre ses infrastructures essentielles. Elle est confiée au centre opérationnel de la sécurité des systèmes d'information. Ce centre est actif 24 heures sur 24. Il assure des fonctions de veille, de détection, d'alerte et de réaction, disposant par exemple de sondes à la frontière des réseaux de l'administration. Il est également en charge de la planification, de la rédaction des plans de réaction et de la conduite d'exercices. Ce centre opérationnel était à la manœuvre en janvier et février lors de l'attaque intervenue contre le ministère de l'Économie et des finances.

Cette attaque a été découverte début janvier 2011, le premier indice étant l'émission d'un courrier électronique depuis un compte de messagerie sans intervention de son titulaire légitime. Pour y répondre, une opération en quatre phases a été mise en place et pilotée par le centre opérationnel de l'ANSSI en liaison étroite avec Bercy et les services de sécurité afin : de comprendre techniquement ce qui s'est passé ; d'identifier l'étendue de l'attaque – Bercy comptant près de 170 000 ordinateurs – ; de nettoyer les réseaux infectés et enfin de sécuriser les systèmes d'information.

Cette opération a mobilisé autour de 30 à 40 personnels de l'ANSSI pendant deux mois, obérant sérieusement sa capacité opérationnelle.

Plus de 150 ordinateurs et autres serveurs ont été compromis. Le niveau technique des procédés utilisés et la mise en œuvre constatée de l'attaque révèlent qu'il s'agit de professionnels déterminés et organisés. Ils étaient méthodiques – revenant régulièrement chercher de nouvelles informations.

Le but des attaquants était, selon toute vraisemblance, de se procurer des informations économiques et financières sur la France, en particulier dans le cadre du G20.

Cependant, savoir traiter les attaques informatiques n'est pas suffisant : il faut que nos systèmes d'information y résistent.

Cet objectif correspond à la deuxième mission de l'agence qui est d'assister et de conseiller les administrations et les grands opérateurs pour sécuriser leurs systèmes d'information.

Elle contribue au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques. Elle est notamment chargée de fournir aux plus hautes autorités de l'État des moyens sécurisés dont le fonctionnement doit être assuré en toutes circonstances.

L'agence vérifie également au travers d'audits et de tests de pénétration le niveau de sécurité des administrations et, demain, des opérateurs.

Enfin, l'agence informe régulièrement les entreprises et le grand public sur les menaces qui pèsent contre les systèmes d'information et sur les moyens de s'en protéger. Elle développe pour cela une politique de communication et de sensibilisation active, par exemple grâce à son portail de la sécurité informatique, inauguré en 2008.

Plus classiquement et pour terminer, l'ANSSI assure la fonction de régulation du secteur de la sécurité des systèmes d'information : relations internationales, définition des règles, avec la définition d'un référentiel général de sécurité, ou encore la labellisation de produits.

L'ANSSI est placée sous l'autorité du Premier ministre et rattachée au secrétariat général de la défense et de la sécurité nationales. Sa gouvernance est assurée par un comité stratégique présidé par le secrétaire général de la défense et de la sécurité nationales.

J'en viens maintenant aux développements les plus récents. À la suite de divers travaux et notamment du dernier exercice Piranet, nous avons été amenés à dresser un certain nombre de constats.

Dans le cas d'une attaque informatique, la réactivité prime. Les attaques informatiques se déplacent à la vitesse du courant électrique, une vitesse proche de celle de la lumière. Dans certaines situations il peut être utile de prendre des décisions rapidement, notamment pour éviter une trop grande infection.

Il faut, y compris pour des raisons juridiques, que l'État identifie clairement une autorité chargée d'édicter les règles au sein de l'administration mais aussi vis-à-vis des opérateurs. Dans cette perspective, le président de la République a décidé l'année dernière que la France se doterait d'une autorité de défense des systèmes d'information. Cette décision s'est concrétisée par le décret du Premier ministre du 11 février 2011, au terme duquel l'ANSSI *« assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité et dans le cadre des orientations fixées par le Premier ministre, elle décide les mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et coordonne l'action gouvernementale.* »

Pour faire court et reprendre une formule de Francis Delon : en cas d'attaque informatique majeure, l'ANSSI prend la main.

Plus récemment, j'ai été conduit à la demande du Gouvernement à dresser un bilan de la situation et à proposer si nécessaire de nouvelles mesures, ce qui a abouti à la communication en conseil des ministres du 25 mai dernier.

Le bilan a démontré que nous étions loin d'avoir résolu le problème, que la menace ne cessait de croître et qu'enfin la situation en France, comme ailleurs dans ce domaine, était inquiétante. Il a donc semblé nécessaire d'accélérer la montée en puissance du dispositif national et de prendre un certain nombre de mesures.

Nous devons en premier lieu renforcer les capacités opérationnelles d'intervention de l'État par la création d'un groupe d'intervention rapide qui se rendra dans les administrations ou chez les opérateurs critiques lorsque des indices laissent à penser qu'ils ont été l'objet d'une attaque informatique particulièrement grave.

Dans le cas où une compromission serait découverte, le groupe d'intervention rapide sera en mesure, à la demande et en appui des équipes de l'administration ou de l'entreprise, d'élaborer les plans de reconstruction des systèmes d'information compromis et de superviser leur mise en œuvre, voire d'y contribuer directement.

Par ailleurs, doté de moyens aptes à être projetés, le groupe d'intervention rapide donnera à la France une capacité d'assistance à ses alliés en cas de crise majeure de nature informatique.

En second lieu, il importe d'augmenter le niveau de sécurité des systèmes d'information de l'État par la mise en place d'une politique interministérielle de sécurité. Chaque administration possède en effet une politique de sécurité, c'est-à-dire un ensemble de règles qui doivent être respectées par les utilisateurs et les informaticiens. L'hétérogénéité des pratiques et des règles de sécurité actuelles nuit gravement à leur compréhension et à leur application. On gagnera beaucoup notamment en lisibilité et en compréhension si tout le monde ou presque applique un ensemble de règles simples, telles que la taille d'un mot de passe et la périodicité de son renouvellement.

La mise en application d'une politique de sécurité commune et la clarification qui en résultera seront de nature à favoriser le respect de ces règles par l'ensemble des agents de l'État.

Par ailleurs, les administrations doivent recourir à des produits et services labellisés par l'ANSSI, c'est-à-dire évalués par le centre d'évaluation de la sécurité des technologies de l'information qui est indépendant.

Nous devons également déployer un intranet interministériel résilient, chaque ministère disposant aujourd'hui de son propre réseau – voire de plusieurs réseaux – avec ses propres passerelles vers l'Internet et de nombreuses passerelles entre ces réseaux.

L'objectif est de permettre la continuité de l'action gouvernementale et administrative en cas de dysfonctionnement grave de l'Internet en limitant le nombre de passerelles d'interconnexion qui sont des points de fragilité potentiels, améliorant ainsi la détection des attaques au niveau des passerelles ainsi que notre capacité à y réagir. Cela permettrait également de réduire les coûts de communications de l'État en rationalisant le nombre de réseaux.

Ce projet sera piloté par Jérôme Filippini, le nouveau directeur interministériel des systèmes d'information et de communication.

Le troisième axe de travail consiste à promouvoir la cybersécurité dans l'enseignement supérieur et la recherche par l'insertion de la sécurité des systèmes d'information dans les formations supérieures, notamment informatiques. En effet, trop d'ingénieurs ou d'universitaires, y compris dans les filières techniques, arrivent aujourd'hui sur le marché du travail sans avoir jamais été formés à « l'hygiène numérique ». Par ailleurs, on ne devrait plus voir un système mis en production avec des mots de passe par défaut encore en place, ou encore des comptes d'installation non désactivés.

Le quatrième axe consiste à améliorer la sécurité des d'infrastructures vitales en établissant un partenariat avec les opérateurs d'infrastructures vitales.

Il s'agit de développer les échanges d'informations entre l'État et les opérateurs critiques, le partage et l'analyse des remontées d'incidents ainsi que les audits de sécurité. Ces évolutions permettront de renforcer la sécurité des systèmes d'information industriels les plus critiques et de veiller à leur défense permanente.

Nous devons notamment créer un réseau d'alerte en cas d'attaque informatique : l'État doit être en mesure de contacter en temps réel les opérateurs d'infrastructures vitales ou les établissements sensibles lorsqu'il a connaissance d'une attaque informatique les visant.

Il en va de même dans l'éventualité d'une découverte de faille de sécurité grave touchant par exemple un système industriel spécifique.

Afin de relever ces différents défis, les moyens de l'ANSSI vont être renforcés pour atteindre 357 personnels en 2013, contre 180 aujourd'hui. Dans le contexte actuel, cette décision permet de mesurer le degré de prise de conscience des autorités sur ce sujet.

M. le président Guy Teissier. La défense nationale a beaucoup investi pour la sécurité de ses systèmes d'information. Est-ce que cet investissement pourrait avoir des effets démultiplicateurs pour les acteurs civils ?

M. Patrick Pailloux. Je vois deux aspects dans votre question.

Premièrement, l'État ne donne pas encore suffisamment l'exemple. C'est pourquoi nous avons souhaité rendre publiques les attaques informatiques dirigées contre Bercy. Les réseaux sont très souvent attaqués. Or, faire la politique de l'autruche nous empêche de mobiliser les moyens nécessaires. Nous devons donc communiquer pour que les entreprises prennent conscience de la menace et se donnent les moyens d'investir dans leur sécurité informatique.

Par ailleurs, la France dispose d'un savoir-faire suffisant, avec des industriels de classe mondiale, une excellente école de cryptologie, parmi les meilleures au monde, une usine de composants informatiques près de Grenoble. L'État doit maintenant inciter les entreprises à se doter de systèmes de sécurité adéquats, d'où le volet sécurité et résilience des réseaux du grand emprunt.

M. Christian Ménard. On a pu observer des similitudes entre les attaques dont Bercy a été récemment l'objet et celle qui a touché le ministère des finances canadien, il y a quelques mois, juste avant la tenue du G 20. Un pays pourrait être à l'origine de ces attaques ? Échangez-vous avec les autres pays en cas d'attaques de ce type ?

M. Michel Grall. Les États-Unis ont indiqué qu'ils pourraient répondre par des moyens militaires conventionnels à une attaque informatique contre leurs systèmes vitaux : quelle est la doctrine de la France en la matière ?

M. Patrick Pailloux. En matière militaire, à ma connaissance la France n'a pas de doctrine définissant une réponse précise à tel ou tel type d'attaque. Je ne peux donc pas proposer de réponse à cette question mais la posture américaine est logique. Les systèmes d'information sont les systèmes nerveux de nos sociétés, une attaque contre ceux-ci peut donc avoir les mêmes conséquences qu'un bombardement. Une réponse militaire n'est donc pas à exclure, en fonction naturellement du type d'attaque.

La France a été victime d'attaques pendant la préparation du G 20, mais elle n'était pas la seule visée. Cela fait plusieurs années que des attaques de ce type sont constatées et elles touchent tous nos alliés. Il faut avoir à l'esprit que les réseaux informatiques ne connaissent pas de frontière. On ignore qui se trouve derrière car il est très difficile de remonter à la source, les pirates utilisant des serveurs différents et un système de rebonds informatiques. Le serveur de commande et de contrôle peut être manipulé d'un ordinateur portable connecté à un réseau Wifi public ou depuis un cybercafé. Il est donc extrêmement difficile de connaître l'identité du donneur d'ordre.

M. Francis Hillmeyer. N'est-il pas plus facile de protéger l'intranet des ministères dès lors que ces systèmes d'information ne sont pas reliés à l'extérieur ? J'aimerais que vous nous parliez aussi des signaux parasites compromettants.

Jean-Jacques Candelier. Le Gouvernement va conforter les moyens de l'ANSSI et je m'en félicite. Le site Internet de la préfecture du Nord a fait l'objet il y a peu d'attaques informatiques : avez-vous des informations sur ce sujet ? Pourquoi attaque-on le site d'une préfecture ? Que mettre en place pour le protéger ? Où en est l'enquête ?

M. Patrick Pailloux. L'ensemble des systèmes d'information des entreprises et administrations est interconnecté. On ne sait plus travailler autrement. Les entreprises sont par exemple très dépendantes de leurs messageries électroniques. On le constate lorsque l'on veut organiser une simulation d'attaque qui supposerait d'en suspendre le fonctionnement pendant quelques heures. Par ailleurs, il n'est pas de système inviolable. La question n'est donc pas d'empêcher les attaques, mais de les détecter rapidement et d'y répondre. Il faut vivre avec cette idée que les attaques sont possibles, et fréquentes.

Des signaux parasites compromettants sont toujours émis par des ordinateurs : le réseau Wifi peut être capté à de très grandes distances.

Les attaques du type de celle subie par la préfecture du Nord sont très fréquentes. Environ 7 000 sites portant un nom de domaine « .fr » sont attaqués en France chaque année, dont plusieurs centaines en « .gouv.fr ». Il s'agit le plus souvent pour nous d'affaires mineures car elles ne concernent que des sites Internet de communication. Nous nous contentons donc de faire des recommandations de sécurité mais nous ne traitons pas au fond le sujet. Je ne peux donc vous faire de réponse détaillée.

M. Dominique Caillaud. J'aimerais revenir sur l'aspect labellisation. Lorsque les ordinateurs portables des entreprises sont détenus par des « inconscients », qui l'oublient dans le train ou l'avion, comment faire pour protéger leurs données ? Existe-t-il des solutions de protection de ces données labellisées sur le marché ?

M. Marc Joulaud. Sur le plan juridique, disposez-vous des moyens suffisants pour demander aux fournisseurs d'accès à Internet de couper le trafic en cas d'attaque majeure ?

M. Patrick Pailloux. La solution miracle assurant une sécurité totale n'existe pas, sauf à imposer de lourdes contraintes aux utilisateurs. Cependant, pour se protéger contre l'espionnage élémentaire ou le vol d'ordinateurs dans les chambres d'hôtel, il existe des solutions qui reposent sur des dispositifs techniques et sur des actions d'éducation des utilisateurs. L'ANSSI a ainsi réalisé un guide pour les hommes d'affaires en voyage réalisé avec le club des directeurs de la sécurité des entreprises. L'ANSSI labellise également des

dispositifs de sécurité. Certaines entreprises sont bien sensibilisées aux risques et utilisent beaucoup ces outils, d'autres moins.

L'ANSSI ne peut pas actuellement donner l'ordre aux fournisseurs d'accès d'effectuer des coupures ou de mettre en place des dispositifs de filtrage, mais cela deviendra possible, en cas de crise majeure, après l'adoption du paquet télécom.

Nous ne disposons pas réellement de statistiques qui permettraient de savoir si nous faisons face à une augmentation des attaques ou si c'est notre capacité à les voir qui progresse. Cependant, il est raisonnable de penser que les attaques à outrance que nous subissons aujourd'hui et qui vont de pair avec l'industrialisation de la profession de pirate ont commencé à se développer il y a deux ou trois ans.

Mme Françoise Hostalier. Je ne suis pas d'accord avec la réponse que vous avez faite à M. Candelier. L'attaque du site de la préfecture du Nord a eu un grand impact sur l'opinion publique.

Je souhaiterais savoir si le désordre qui peut exister dans le domaine de l'informatique, et notamment la multiplicité des acteurs, peut constituer une protection contre d'éventuelles attaques.

Par ailleurs, ne pourrait-on pas imaginer que des terroristes prennent un jour le contrôle du système informatique d'infrastructures vitales telles que des centrales nucléaires ?

M. Daniel Boisserie. Au niveau international, la cyberguerre est-elle reconnue comme une agression miliaire ? Par ailleurs, avez-vous les moyens de riposter à une attaque étrangère dans ce domaine ?

M. Patrick Pailloux. De fait une cyberattaque (volontaire ou non) dirigée contre un hôpital (ce qui a déjà eu lieu) est plus grave qu'une attaque dirigée contre le site d'une préfecture. Dans un hôpital, le simple fait qu'une personne introduise une clé USB contenant un virus dans une unité centrale peut infecter tout le réseau et rendre impossible le fait de pratiquer des analyses de sang ou de faire des radios.

Les infrastructures vitales reposent, en matière informatique, sur des technologies rustiques, ce qui peut les mettre à l'abri d'attaques. Cependant, ces technologies rustiques sont progressivement remplacées par la technologie IP et risquent alors de devenir, progressivement, vulnérables à des attaques menées à partir de l'Internet.

Le désordre, en matière informatique, peut être une protection contre les attaques si on multiplie les technologies. Mais, d'une façon générale, l'ordre vaut mieux que le désordre en la matière. En effet, un agent qui passe d'une administration où il y a une politique de sécurité, en ce qui concerne par exemple les mots de passe, à une administration où il n'y en a pas risque de se sentir perdu.

L'ANSSI a une vocation exclusivement défensive. Cependant, le Livre blanc prévoit que le président de la République puisse disposer de capacités offensives dans le cyberespace en cas de conflit armé, mais elles relèvent alors des forces armées.

À l'échelle internationale, un cycle de discussions stratégiques va débuter en novembre sur la question de savoir s'il faut un droit du cyberespace.

M. Philippe Folliot. L'Estonie est le pays qui a connu les attaques les plus importantes au point d'être particulièrement déstabilisé à cette occasion. Avez-vous été en contact à ce sujet avec les autorités estoniennes ?

Par ailleurs, qu'en est-il de la Chine, que l'on soupçonne d'abriter des officines menant des cyberattaques ?

Mme Michèle Alliot-Marie. Quels sont les États les mieux équipés en matière de protection des systèmes d'information ? Quelle coopération existe dans ce domaine au plan international ? Quel est le degré de confiance en la matière entre les pays européens ? Une action est-elle menée au niveau européen en matière de protection ?

M. Patrick Pailloux : Il y a eu un retour d'expérience détaillé concernant l'affaire de l'Estonie. Un accord de coopération a d'ailleurs été signé par la France avec ce pays en novembre dernier. La principale faille de l'Estonie dans le domaine de la cyber-sécurité, est qu'il s'agit de l'un des pays utilisant le plus Internet. Le conseil des ministres lui-même est retransmis en direct sur la toile.

La menace grandit au fur et à mesure que l'on s'interconnecte. Les moyens utilisés contre l'Estonie étaient extrêmement simples et il s'agissait d'une attaque élémentaire. Elle n'a coûté que quelques centaines de dollars par jour, ne mobilisant que quelques milliers de machines seulement.

Les États les mieux équipés doivent plutôt être considérés comme les États les moins en retard. Ainsi les États-Unis sont en pointe, mais ils restent extrêmement fragiles et ils le reconnaissent eux-mêmes.

En Europe, le Royaume-Uni et l'Allemagne sont les pays ayant le mieux pris la mesure de la situation. Néanmoins aucun État n'est significativement plus protégé que les autres. Les Britanniques viennent d'annoncer un programme d'investissement de 650 millions de livres sterling dans le domaine de la cyber-défense.

Historiquement il y avait peu d'échanges internationaux dans le domaine de la défense des systèmes d'information, chacun gardant jalousement secret ses propres dispositifs. Cependant, la situation a beaucoup évolué dans ce domaine : nous subissons tous les mêmes attaques venant a priori des mêmes commanditaires, difficiles à détecter. La coopération dans ce domaine est, par exemple, explicitement mentionné dans l'accord de défense signé avec le Royaume-Uni en novembre dernier. Les coopérations bilatérales sont assez efficaces, mais elles en sont à leurs prémices.

La situation est plus complexe sur le plan multilatéral. Elle n'est que très peu développée, sauf peut-être dans des domaines très techniques, tels que l'échange de signatures virales ou d'adresses IP malveillantes.

L'action européenne a évolué dans le bon sens. Il existe une agence européenne – l'ENISA *(European Network and Information Security Agency*) –, basée à Héraklion, et dont l'efficacité va croissant. L'engagement communautaire peut se déployer selon deux axes.

Étant mutuellement dépendants, avec des systèmes très intégrés, nous devons veiller à ce que chaque pays de l'Union dispose d'un niveau minimum de sécurité. Il faut donc aider nos partenaires les moins bien dotés à s'équiper d'une capacité de défense.

La deuxième dimension de l'action européenne concerne la résilience des réseaux. L'ensemble de la réglementation dans ce domaine est décidé à Bruxelles et celle-ci est relativement pauvre en matière de sécurité. Mais les choses sont en train d'évoluer. Par exemple, la transposition du paquet télécom comprend une obligation de déclaration d'incident.

La séance est levée à 11 heures 15.

*
* *

Membres présents ou excusés

Présents. — Mme Patricia Adam, Mme Michèle Alliot-Marie, Mme Marie-Noëlle Battistel, M. Jean-Louis Bernard, M. Daniel Boisserie, Mme Françoise Briand, M. Pascal Brindeau, M. Dominique Caillaud, M. Jean-Jacques Candelier, M. Guy Chambefort, M. François Cornut-Gentille, M. Bernard Deflesselles, M. Lucien Degauchy, M. Jacques Desallangre, M. Jean-Pierre Dupont, M. Philippe Folliot, M. Michel Grall, M. Francis Hillmeyer, Mme Françoise Hostalier, M. Marc Joulaud, M. Alain Marleix, M. Christian Ménard, M. Damien Meslot, M. Jean Michel, M. Jean-Claude Perez, M. Alain Rousset, M. Guy Teissier, M. Yves Vandewalle, M. Jean-Claude Viollet, M. Michel Voisin

Excusés. — M. Laurent Cathala, M. Bernard Cazeneuve, M. Laurent Fabius, M. Pierre Frogier, M. Guillaume Garot, M. André Gerin, M. Franck Gilard, Mme Marguerite Lamour, M. Jean-Marie Le Guen, Mme Martine Lignières-Cassou, M. Daniel Mach, M. Franck Marlin, M. Georges Mothron, M. Alain Moyne-Bressand, M. Philippe Nauche, M. Gwendal Rouillard, M. Philippe Vitel, M. André Wojciechowski