N° 681

SÉNAT

SESSION EXTRAORDINAIRE DE 2011-2012

Enregistré à la Présidence du Sénat le 18 juillet 2012

RAPPORT D´INFORMATION

FAIT

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la **cyberdéfense**,

Par M. Jean-Marie BOCKEL,

Sénateur.

(1) Cette commission est composée de : M. Jean-Louis Carrère, *président ;* MM. Didier Boulaud, Christian Cambon, Jean-Pierre Chevènement, Robert del Picchia, Mme Josette Durrieu, MM. Jacques Gautier, Robert Hue, Xavier Pintat, Yves Pozzo di Borgo, Daniel Reiner, *vice-présidents ;* Mmes Leila Aïchi, Hélène Conway Mouret, Joëlle Garriaud-Maylam, MM. Gilbert Roger, André Trillard, *secrétaires ;* MM. Pierre André, Bertrand Auban, Jean-Michel Baylet, René Beaumont, Pierre Bernard-Reymond, Jacques Berthou, Jean Besson, Michel Billout, Jean-Marie Bockel, Michel Boutant, Jean-Pierre Cantegrit, Pierre Charon, Marcel-Pierre Cléach, Raymond Couderc, Jean-Pierre Demerliat, Mme Michelle Demessine, MM. André Dulait, Hubert Falco, Jean-Paul Fournier, Pierre Frogier, Jacques Gillot, Mme Nathalie Goulet, MM. Alain Gournac, Jean-Noël Guérini, Joël Guerriau, Gérard Larcher, Robert Laufoaulu, Jeanny Lorgeoux, Rachel Mazuir, Christian Namy, Alain Néri, Jean-Marc Pastor, Philippe Paul, Jean-Claude Peyronnet, Bernard Piras, Christian Poncelet, Roland Povinelli, Jean-Pierre Raffarin, Jean-Claude Requier, Richard Tuheiava, André Vallini.

SOMMAIRE

Pages

LES 10 PRIORITÉS DU RAPPORT

Priorité n°1 : Faire de **la cyberdéfense** et de la **protection des systèmes d'information une priorité nationale**, portée **au plus haut niveau de l'Etat**, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. S'interroger sur la pertinence de formuler une **doctrine publique** sur **les capacités offensives** ;

Priorité n°2 : Renforcer **les effectifs, les moyens et les prérogatives** de **l'Agence nationale de sécurité des systèmes d'information**, ainsi que les effectifs et les moyens dédiés au sein **des armées, de la direction générale de l'armement et des services spécialisés**, et développer **une véritable politique des ressources humaines** ;

Priorité n°3 : Introduire des **modifications législatives** pour donner les moyens à l'ANSSI d'exercer ses missions et instituer **un pôle juridictionnel spécialisé à compétence nationale** pour réprimer les atteintes graves aux systèmes d'information ;

Priorité n°4 : Améliorer la prise en compte de **la protection des systèmes d'information dans l'action de chaque ministère**, en renforçant la sensibilisation à tous les niveaux, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse permettant de détecter les attaques, ainsi qu'en rehaussant l'autorité des fonctionnaires de sécurité des systèmes d'information ;

Priorité n°5 : Rendre **obligatoire** pour les entreprises et les opérateurs d'importance vitale **une déclaration d'incident** à l'ANSSI en cas d'attaque importante contre les systèmes d'information et encourager **les mesures de protection** par des mesures incitatives ;

Priorité n°6 : Renforcer la protection des systèmes d'information des **opérateurs d'importance vitale**, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse, en généralisant les audits, en rendant obligatoire la déclaration des processus et automates industriels connectés à Internet et en favorisant la mise en place, de manière sectorielle, de centres de détection communs ;

Priorité n°7 : Soutenir par **une politique industrielle volontariste**, à l'échelle nationale et européenne, le tissu industriel des entreprises françaises, notamment des PME, spécialisées dans la conception de certains **produits ou services importants pour la sécurité informatique** et, plus largement, du **secteur des technologies de l'information et de la communication**, et renforcer la coopération entre l'Etat et le secteur privé ;

Priorité n°8 : Encourager **la formation d'ingénieurs spécialisés** dans la protection des systèmes d'information, développer **la recherche** et les **activités de conseil**, et accentuer **la sensibilisation du public**, notamment au moyen d'une campagne de communication inspirée de la prévention routière ;

Priorité n°9 : Poursuivre **la coopération bilatérale** avec nos principaux alliés, soutenir l'action de **l'OTAN** et de **l'Union européenne**, engager **un dialogue** avec la Chine et la Russie et promouvoir l'adoption **au niveau international** de mesures de confiance ;

Priorité n°10 : Interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de **« routeurs » ou d'autres équipements de cœur de réseaux** qui présentent **un risque pour la sécurité nationale, en particulier les « routeurs » et certains équipements d'origine chinoise.**

« (…) un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières »

Qiao Liang et Wang Xiangsui

La guerre hors limites, Payot et Rivages, 1999, p.58.

Mesdames, Messieurs,

Le Livre blanc sur la défense et la sécurité nationale de 2008 avait déjà identifié les attaques contre les systèmes d'information comme l'une des **principales menaces qui pèsent sur notre défense et notre sécurité**.

D'après les rédacteurs du Livre blanc : *« **Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner**. Or, le « cyberespace », constitué par le maillage de l'ensemble des réseaux, est radicalement différent de l'espace physique : sans frontière, évolutif, anonyme, l'identification certaine d'un agresseur y est délicate.*

La menace est multiforme : blocage malveillant, destruction matérielle (par exemple de satellites ou d'infrastructures de réseau névralgiques), neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles.

*Dans les quinze ans à venir, la **multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude**. Certaines d'entre elles pourront être de grande ampleur ».*

Aujourd'hui, le sentiment qui prédomine est que **l'ampleur de la menace a été largement sous-estimée.**

Comme le relève le document préparatoire à l'actualisation du Livre blanc, publié en février 2012, *« **depuis 2008, les risques et les menaces qui pèsent sur le cyberespace se sont nettement confirmés**, à mesure que celui-ci devenait un champ de confrontation à part entière avec la montée en puissance rapide du cyber espionnage et la multiplication des attaques informatiques en direction des Etats, des institutions ou des entreprises. Les risques identifiés par le Livre blanc comme étant de long terme se sont donc en partie déjà concrétisés et **la menace atteint désormais un niveau stratégique** ».*

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, **il ne se passe pratiquement pas une semaine sans que l'on annonce, quelque part dans le monde, une attaque informatique importante contre de grandes institutions, publiques ou privées**, qu'il s'agisse de cybercriminalité ou d'espionnage informatique.

La France n'est pas épargnée par ce phénomène, puisque notre pays a été victime de plusieurs attaques informatiques d'envergure, à l'image de **l'attaque contre les systèmes d'information du ministère de l'économie et des finances**, découverte fin 2010 à la veille de la présidence française du G8 et du G20, ou encore de **l'affaire**, révélée par la presse, **d'espionnage via l'Internet du groupe AREVA**.

Tout récemment, la presse a révélé que même **la Présidence de la République** aurait fait l'objet d'une ou de plusieurs attaque(s) informatique(s) de grande ampleur[1]. Pour sa part, votre rapporteur considère que, si ces attaques sont avérées, **la Présidence de la République devrait le reconnaître officiellement et communiquer publiquement sur ce sujet** car il ne sert à rien de vouloir le cacher ou chercher à minimiser les faits. Au contraire, **votre rapporteur considère qu'il serait souhaitable que les grandes institutions qui ont été victimes d'attaques informatiques communiquent publiquement sur le sujet**, naturellement une fois que ces attaques ont été traitées. C'est d'ailleurs ce que font les autorités américaines ou britanniques. En effet, c'est à ses yeux le meilleur moyen de sensibiliser les administrations, les entreprises ou les utilisateurs à l'importance de ces enjeux.

Par ailleurs, les révélations du journaliste américain David E. Sanger sur l'origine du **virus STUXNET**, qui a gravement endommagé des centrifugeuses du site d'enrichissement d'uranium de Natanz, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran, ou encore la découverte récente du **virus FLAME**, vingt fois plus puissant, laissent présager l'apparition de nouvelles « armes informatiques » aux potentialités encore largement ignorées.

Dans ce contexte, **la France est-elle suffisamment préparée pour se protéger et se défendre face aux attaques informatiques ?**

Dans un rapport de 2006 remis au Premier ministre, notre ancien collègue député M. Pierre Lasbordes dressait un constat sans complaisance des faiblesses de notre organisation et de nos moyens, notamment au regard de nos partenaires européens les plus proches.

En février 2008, dans un rapport d'information présenté au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, notre ancien collègue sénateur M. Roger Romani estimait que *« la France n'est ni bien préparée, ni bien organisée »* face à cette menace.

---

[1] *Voir l'article de M. Jean Guisnel, « Cyber-attaques. L'appareil d'Etat visé », Le télégramme, 11 juillet 2012*

Depuis 2008, les choses ont beaucoup évolué. Grâce à l'impulsion donnée par **le Livre blanc de 2008**, **une agence nationale de la sécurité des systèmes d'information** a été instituée et notre pays s'est doté d'une **stratégie nationale** dans ce domaine.

Pour autant, **la persistance, voire l'augmentation des attaques informatiques constatées ces dernières années en France** semble montrer qu'il reste encore d'importants efforts à accomplir pour renforcer la protection des systèmes d'information des administrations, des entreprises ou des opérateurs d'importance vitale et pour sensibiliser l'ensemble des acteurs.

C'est la raison pour laquelle la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat a jugé utile, à la veille de l'élaboration du nouveau Livre blanc et de la future Loi de programmation militaire, de se pencher à nouveau sur ce sujet et a confié à votre rapporteur en octobre dernier la mission de rédiger un rapport sur la cyberdéfense.

Pour ce faire, votre rapporteur a eu de nombreux entretiens avec les principaux responsables chargés de la protection et de la défense des systèmes d'information au sein de l'Etat, des services de renseignement et des armées, avec des représentants des entreprises ou des experts[1].

Afin d'avoir une vue comparative, votre rapporteur s'est également rendu aux Etats-Unis, au Royaume-Uni, en Allemagne et en Estonie, ainsi qu'à Bruxelles au siège de l'OTAN et auprès des institutions européennes, pour mesurer le rôle de l'OTAN et de l'Union européenne sur ce dossier.

A cet égard, votre rapporteur tient à remercier l'ensemble des personnalités rencontrées en France ou à l'étranger, pour leur disponibilité et leur aide précieuse dans l'élaboration de ce rapport.

Votre rapporteur exprime aussi sa gratitude aux Ambassadeurs de France et à leurs collaborateurs de nos représentations diplomatiques à Washington, à Londres, à Berlin, à Tallin et à Bruxelles, auprès de l'OTAN et de l'Union européenne, pour leur soutien dans l'organisation et le bon déroulement de ses déplacements, ainsi qu'au *German Marshall Fund*, pour son aide dans l'organisation de sa visite aux Etats-Unis.

Après avoir présenté un rapport d'étape devant votre commission[2], votre rapporteur a souhaité donner dans ce rapport une vue aussi complète et objective que possible de **l'état de la menace** et **des efforts réalisés par nos partenaires pour y faire face**, afin de **mesurer l'efficacité du dispositif** mis en place par notre pays, ses **lacunes éventuelles** et **les moyens d'y remédier**.

Dans l'optique de l'élaboration du nouveau Livre blanc, votre rapporteur a également pensé utile de formuler des **priorités** et des **recommandations concrètes** pour renforcer notre dispositif.

---

[1] *La liste des personnalités rencontrées figure en annexe au présent rapport*

[2] *Voir la communication de votre rapporteur devant la commission des affaires étrangères, de la défense et des forces armées du Sénat en date du 22 février 2012*

En effet, comme l'indique la lettre de mission adressée par le Président de la République, le 13 juillet dernier, à M. Jean-Marie Guehenno, relative à la constitution de la commission chargée de rédiger le nouveau Livre blanc sur la défense et la sécurité nationale, parmi les principales menaces susceptibles de peser sur la sécurité nationale dans les quinze à vingt années à venir figurent les attaques contre les systèmes d'information, d'origine étatique ou non. Pour le Président de la République, il convient donc d'en tenir compte dans le cadre des réflexions qui devraient déboucher sur l'élaboration d'un nouveau Livre blanc au début de l'année 2013.

Mais, avant toute chose, **que faut-il entendre par « cyberdéfense » ?**

On entend souvent employer indistinctement les termes de *« cybersécurité »*, de *« cybercriminalité »*, voire de *« cyberguerre »*.

Aux yeux de votre rapporteur, la *« cyberdéfense »* est une notion complémentaire de la *« cybersécurité »*, qui englobe la protection des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense.

Pour reprendre la définition de l'agence nationale de sécurité des systèmes d'information, elle désigne l'*« ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels »*.

Elle se distingue en particulier de la lutte contre la *« cybercriminalité »*, qui recouvre un champ très vaste et que votre rapporteur a volontairement choisi d'écarter de sa réflexion pour se concentrer sur les **attaques informatiques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation et les moyens de s'en protéger.**

I. LES ATTAQUES CONTRE LES SYSTÈMES D'INFORMATION : UNE MENACE STRATÉGIQUE QUI S'EST CONCRÉTISÉE ET ACCENTUÉE AU COURS DE CES DERNIÈRES ANNÉES

Avec le développement considérable de l'Internet et des nouvelles technologies, les systèmes d'information et de communication occupent désormais une place centrale dans le fonctionnement nos sociétés. Or, il apparaît aujourd'hui que le développement des systèmes d'information et de communication et leur interconnexion croissante, dans toutes les formes d'activités, ont souvent été réalisés au détriment des exigences de sécurité qui constituent en la matière une contrainte incontestable.

Comme le rappelle M. Roger Romani dans son excellent rapport, *« la vulnérabilité des réseaux informatiques n'est pas une préoccupation récente. C'est en 1988 que le premier « ver » informatique est apparu sur l'Internet qui connaissait alors ses premiers développements. Depuis lors, particuliers, entreprises ou institutions se sont familiarisés avec le risque de propagation de « virus » altérant, parfois gravement, le fonctionnement des systèmes informatiques, ou encore la prolifération des courriers électroniques indésirables, les spams, dont certains visent à obtenir frauduleusement les identifiants de connexion ou les coordonnées bancaires de l'utilisateur »*

Par rapport à d'autres modes d'action, comme l'espionnage ou la destruction physique, le recours à une attaque informatique présente de nombreux avantages, car il s'avère **moins risqué**, **moins coûteux** et **beaucoup plus discret**, l'identification de son auteur étant extrêmement difficile. Par ailleurs, il est complexe de se protéger contre les attaques informatiques, car les techniques évoluent sans cesse et il n'existe pas de parade absolue dans le « cyberespace ». Autre difficulté, la sécurité informatique est largement dépendante des comportements des utilisateurs des systèmes d'information, qui considèrent souvent les règles de sécurité comme autant de contraintes.

Si les risques soulevés par la « cybercriminalité » sur l'économie avaient déjà été identifiés depuis longtemps, la perception d'un risque pesant plus particulièrement sur la sécurité des Etats est plus récente.

Elle recouvre principalement **deux types** de préoccupations. La première porte sur les **services essentiels au fonctionnement du pays ou à sa défense**, tributaires de systèmes d'information qui pourraient être visés par des attaques tendant à les paralyser. La seconde concerne la **protection des informations sensibles** du point de vue politique, militaire ou économique, face à des techniques d'intrusion informatique de plus en plus sophistiquées.

Avant de tenter de dresser une typologie des attaques informatiques, des méthodes utilisées et des cibles potentielles, votre rapporteur a souhaité revenir brièvement sur plusieurs affaires, ailleurs dans le monde et en France, qui ont mis en lumière l'importance prise aujourd'hui par les attaques contre les systèmes d'information.

A. DE TALLIN À TÉHÉRAN : AUCUN PAYS N'EST AUJOURD'HUI À L'ABRI DES ATTAQUES INFORMATIQUES

Ces dernières années, un grand nombre d'organisations, d'Etats ou d'entreprises partout dans le monde ont été victimes d'attaques informatiques.

Votre rapporteur a souhaité illustrer ces attaques par trois exemples qui montrent bien la très grande diversité des cibles et des méthodes utilisées.

1. Le cas de l'Estonie : une perturbation massive de la vie courante d'un pays

Les attaques informatiques ont constitué l'une des manifestations de la **crise survenue en Estonie à la fin du mois d'avril 2007**, à la suite de la décision des autorités de déplacer le monument érigé en souvenir des combattants de l'armée soviétique qui avaient mis fin à l'occupation allemande en 1944, du centre de la capitale vers un cimetière militaire. Cette décision fut vigoureusement contestée par le gouvernement russe, et en Estonie même, par la communauté russophone qui représente près de 30 % de la population.

Le 27 avril 2007, au lendemain du déplacement du monument, démarrait une **vague d'attaques informatiques visant les sites Internet gouvernementaux et publics, ceux des opérateurs de téléphonie mobile, des banques commerciales et des organes d'information**.

Ces attaques par « **déni de service distribué »** (*Distributed denial of service – DDoS*) visaient à **saturer, par une multitude de demandes de connexions simultanées, les sites concernés**. Ceux-ci se trouvaient de ce fait inaccessibles. Les perturbations se sont poursuivies pendant près d'un mois et demi, mais elles ont culminé le 9 mai, journée au cours de laquelle 58 sites furent rendus indisponibles, certains d'entre eux ayant fait l'objet de plus de 5 millions de tentatives de connexions par seconde.

Il faut savoir que l'Estonie figure parmi les pays du monde dans lesquels l'usage de l'Internet est le plus répandu, beaucoup de services n'étant accessibles qu'en ligne, notamment les services bancaires (95 % des opérations bancaires s'effectuent par communication électronique).

Si ces attaques n'ont pas directement porté atteinte aux systèmes informatiques internes du gouvernement ni à ceux du secteur privé, et notamment des banques, elles ont **perturbé de manière spectaculaire le fonctionnement de la vie courante du pays**, en privant les usagers de l'accès à certains services en ligne essentiels.

Elles ont également surpris par leur soudaineté, leur ampleur et leur caractère coordonné, ce qui conduit à exclure la seule action d'individus isolés agissant par motivation politique et utilisant des moyens disponibles sur certains sites Internet.

La particularité de telles attaques est qu'il est **très difficile d'en identifier les commanditaires**. En effet, la technique utilisée pour ces attaques est celle des « réseaux de machines zombies **»** (*botnets*) constitués d'ordinateurs compromis à l'insu de leur propriétaire, et contrôlés par l'auteur de l'attaque. On ne peut donc en aucun cas se fier à la provenance apparente des envois, puisqu'ils émanent d'ordinateurs qui échappent au contrôle de leur utilisateur légitime.

Le contexte politique et le fait qu'un grand nombre de communications provenaient de Russie ont conduit les autorités estoniennes à évoquer une action menée par les services de renseignement russes, ce que Moscou a immédiatement démenti. L'Estonie a d'ailleurs sollicité l'aide de la Russie pour identifier la provenance de ces attaques mais elle s'est heurtée à une fin de non recevoir de la part de Moscou. Seul un jeune étudiant estonien russophone a été identifié comme ayant pris part aux attaques et condamné.

Le cas estonien illustre bien l'utilisation qui peut être faite de l'attaque par déni de service à titre d'intimidation ou de représailles dans un contexte de tensions politiques.

Votre rapporteur avait déjà eu l'occasion, en tant que Secrétaire d'Etat à la Défense, de rencontrer les membres du gouvernement estonien au printemps 2008, dans le cadre de la préparation de la présidence française de l'Union européenne, et il avait pu se rendre compte du profond traumatisme de la population à la suite de cette attaque.

Lors d'un déplacement à Tallin, le 28 mai 2012, à l'occasion de la session de printemps de l'assemblée parlementaire de l'OTAN, votre rapporteur a pu mesurer **l'importance accordée à la cyberdéfense par les autorités estoniennes depuis cette affaire**. Le Président de la République et le ministre estonien de la défense ont, en effet, consacré une part importante de leur intervention devant l'assemblée parlementaire de l'OTAN à cette question et notamment au rôle de l'OTAN en matière de cyberdéfense.

Votre rapporteur a pu également s'entretenir avec le secrétaire général du ministère de la défense estonien, ainsi qu'avec le directeur de l'agence estonienne pour la sécurité des systèmes d'information.

Dès 2008, l'Estonie s'est dotée d'une stratégie de cyberdéfense et a créé une agence nationale de la sécurité des systèmes d'information. Cette agence, qui dépendait auparavant du ministère de la défense, mais qui est aujourd'hui placée sous l'autorité du ministère de l'économie et des communications, et qui compte 80 personnes, exerce un rôle opérationnel, joue un rôle de planification et de supervision. Ses attributions ont été renforcées en juin 2011. 142 entreprises ou opérateurs d'importance stratégiques ont été identifiés et la législation estonienne prévoit l'obligation, sous peine d'amende, pour ces entreprises ou opérateurs, de notifier les incidents informatiques importants à l'agence. L'agence est également chargée d'aider les différentes administrations à renforcer la protection de leurs systèmes d'information et émet des recommandations et des conseils.

Les autorités estoniennes attachent aussi une grande importance à la coopération internationale. L'agence estonienne et l'agence nationale française de sécurité des systèmes d'information ont d'ailleurs signé en 2010 un accord de coopération.

2. STUXNET : une « arme informatique » des Etats-Unis dirigée contre le programme nucléaire militaire iranien ?

Le virus informatique STUXNET a été découvert en juin 2010 par la société biélorusse spécialisée dans les produits de sécurité informatique VirusBlokAda.

Les autorités iraniennes révèlent alors qu'elles ont été victimes d'une vaste attaque informatique visant leurs installations nucléaires. STUXNET aurait, en effet, endommagé le réacteur de la centrale nucléaire de Busher et détruit un millier de centrifugeuses du site d'enrichissement d'uranium de Natanz. Selon certaines sources, cette attaque aurait permis de retarder de six mois à deux ans, le programme nucléaire militaire de l'Iran.

Décrit à l'époque comme *« l'arme cybernétique la plus sophistiquée jamais déployée »*[1] ou comme une *« cyber arme de destruction massive »* **STUXNET est un virus informatique qui a été calibré pour s'attaquer à un logiciel informatique bien spécifique**, mis au point par Siemens et utilisé dans différentes installations industrielles. Il s'agit de ce que les spécialistes appellent un SCADA (*Supervisory, control and data acquisition*), c'est-à-dire un système de contrôle et de supervision de processus industriels, utilisé dans des domaines tels que la distribution d'énergie ou la régulation des transports.

Si de tels systèmes ne sont généralement pas reliés directement à l'Internet, il suffit d'introduire – volontairement ou non - un tel virus dans le système par exemple grâce à une clé USB infectée.

Présent dans le système, le ver « reniflerait » d'abord le système d'exploitation et ne s'attaquerait à celui-ci que si celui-ci correspond aux critères de cible, rendant de ce fait sa détection difficile. Une fois sa cible repérée, STUXNET reprogramme le SCADA afin de saboter l'installation industrielle.

Dans le cas iranien, ce programme malveillant a ciblé les centrifugeuses du site d'enrichissement d'uranium de Natanz, en modifiant leur vitesse de rotation jusqu'à ce qu'elles soient hors d'usage. **Il aurait ainsi détruit environ un millier de centrifugeuses sur cinq mille**. Ces dégâts ont été observés par l'Agence internationale de l'énergie atomique (AIEA) au moment où le site était en activité. Parallèlement, il a perturbé les systèmes numériques d'alerte, d'affichage et d'arrêt, qui contrôlent les centrifugeuses, rendant de ce fait ces systèmes aveugles à ce qui se passait.

---

[1] *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay" par William J. Broad, John Markoff et David E. Sanger, publié dans le journal "The New York Times", 15 janvier 2011*

A la suite d'une erreur de manipulation, STUXNET se serait répandu sur l'Internet, infectant plus de 100 000 ordinateurs dans le monde, dont plus de la moitié situés en Iran, permettant ainsi de l'identifier.

Si de forts soupçons pesaient déjà sur les Etats-Unis et Israël, ces intuitions ont été confirmées par **les révélations du journaliste américain David E. Sanger** dans un article du *New York Times* du 1er juin et dans un ouvrage publié le 5 juin dernier[1], intitulé *« Confront and Conceal : Obama's Secret Wars »*.

Dans son livre, particulièrement bien documenté, David E. Sanger décrit en détail comment STUXNET aurait été conçu puis utilisé par l'agence américaine de sécurité nationale (NSA), avec la collaboration de l'armée israélienne (dont l'unité 8 200 de *Tsahal*), dans le cadre d'une opération baptisée *« Olympic Games »* (« Jeux Olympiques »). Initiée par le Président George W. Bush en 2006 et intensifiée ensuite par le Président Barack Obama, cette opération aurait été dirigée contre le programme nucléaire militaire de l'Iran.

Même si les autorités américaines n'ont pas confirmé ces révélations, la première réaction de l'administration présidentielle a été d'ouvrir une enquête criminelle pour identifier les auteurs de la fuite, ce que certains journalistes ont interprété comme un aveu implicite.

La publication du livre de David E. Sanger, en pleine campagne présidentielle, a soulevé une vaste polémique aux Etats-Unis, qui curieusement portait moins sur la légitimité, au regard du droit international, de développer et d'utiliser des « cyberarmes » à l'encontre d'un autre Etat, et d'encourager ainsi les « pirates informatiques », d'autres organisations ou Etats à se doter et à utiliser de telles armes informatiques, que sur les origines de cette fuite.

Pour l'ancien directeur de la CIA, Michael Hayden, STUXNET *« est la première attaque majeure de cette nature qui parvient à entraîner des destructions physiques affectant une infrastructure importante (…). Quelqu'un a franchi le Rubicon. Je ne veux pas dire que nous allons assister aux mêmes conséquences, mais, d'une certaine manière, nous sommes un petit peu en août 1945 »*.

3. **FLAME : un vaste dispositif d'espionnage informatique ?**

Le 28 mai 2012, l'éditeur russe de logiciels anti-virus Kaspersky Lab a annoncé dans un communiqué avoir identifié un nouveau virus informatique, vingt fois plus puissant que STUXNET, baptisé FLAME[2].

---

[1] *David E. Sanger, « Confront and Conceal : Obama's Secret Wars and Surprising Use of American Power", Crown Publishing Group, 5 juin 2012*

[2] *Voir notamment l'article d'Yves Eudes « FLAME virus espion d'Etat » paru dans le journal Le Monde du 20 juin 2012*

L'affaire a débuté lorsqu'au début du mois de mai, l'Union internationale des télécommunications (UIT), institution spécialisée des Nations Unies, a été sollicitée par plusieurs pays du Moyen-Orient dont les installations pétrolières avaient subi des attaques informatiques massives ayant abouti au vol et à l'effacement soudain d'un nombre élevé de données stockées dans leurs systèmes d'information. Ainsi, en avril dernier, à la suite de l'infection par un logiciel malveillant particulièrement sophistiqué, les autorités iraniennes avaient été contraintes d'interrompre la connexion à l'Internet du réseau informatique du terminal de l'île de Kharg, par lequel transitent environ 90 % des exportations du pétrole iranien.

Mandatée par l'UIT, la société russe Kapsersky Lab, ainsi que le laboratoire hongrois CrySys de l'université de technologie de Budapest, découvrent alors un virus informatique d'une puissance jusqu'alors inédite.

A la différence de STUXNET, qui visait à entraver et à détruire le fonctionnement des systèmes de type SCADA, **FLAME serait un type très complexe de logiciel malveillant visant à infiltrer un ordinateur à l'insu de son utilisateur pour en prendre le contrôle, collecter des informations ou effacer des fichiers.**

FLAME serait ainsi un logiciel malveillant conçu à des fins d'espionnage, **vingt fois** plus volumineux que STUXNET[1] et **cent fois** plus qu'un logiciel malveillant « classique », dont *« la complexité et la fonctionnalité dépassent toutes les autres cybermenaces connues à ce jour »*.

Selon les spécialistes, il serait comparable à une **« boîte à outils »**, comprenant une large panoplie de logiciels ayant chacun leur spécialité, qui travailleraient en secret, sans perturber le fonctionnement de l'ordinateur. Il serait en mesure d'identifier et de recopier n'importe quel type de fichier, de lire les courriels, de mémoriser chacune des frappes sur le clavier, de réaliser des captures d'écran, d'enregistrer les conversations et de filmer l'environnement en activant lui-même le micro de l'ordinateur ou la webcam. Il serait même capable de déclencher l'émetteur-récepteur sans fil pour communiquer avec des ordinateurs portables ou des ordiphones situés à proximité.

FLAME viserait en premier lieu les ordinateurs équipés du système d'exploitation Windows de Microsoft. Grâce à des certificats de sécurité fabriqués à l'aide de vulnérabilités dans des algorithmes cryptographiques, il se ferait passer pour une mise à jour de Windows. Contrairement à STUXNET, il ne se propagerait pas automatiquement sur le réseau, mais seulement au coup par coup, sur décision d'un « serveur de commande et de contrôle », afin d'éviter une prolifération anarchique qui augmenterait le risque de détection. Une quinzaine de ces serveurs de commande et de contrôle auraient été identifiés, notamment en Europe et en Asie. Certains spécialistes estiment que FLAME serait actif depuis au moins deux ans mais

[1] *Le volume du virus FLAME serait de 20 méga-octets, contre 1 méga-octet pour STUXNET*

d'autres évoquent une période plus longue, de cinq ans. Avant de transmettre les données collectées aux serveurs de commande et de contrôle, le virus FLAME sécuriserait ses communications, grâce à un chiffrement intégré. Une autre particularité du virus FLAME tiendrait au fait qu'il serait doté d'une fonction « suicide » : dès qu'il aurait rempli sa mission, il s'autodétruirait.

Le 10 juin dernier, la société américaine de sécurité informatique Symantec a assuré que le virus FLAME avait reçu l'ordre de *« disparaître sans laisser de trace »*.

D'après la société Kaspersky, plus de 1000 ordinateurs auraient été recensés comme infectés, début juin, principalement dans les pays du Proche et du Moyen Orient, notamment en Iran, dans les territoires palestiniens, en Syrie, au Liban, en Arabie Saoudite, aux Emirats arabes unis et en Égypte, mais aussi au Soudan ou dans d'autres pays. Des traces de FLAME ont été découvertes sur des ordinateurs situés dans des administrations, des opérateurs ou des entreprises, des universités, mais aussi sur des ordinateurs personnels de cadres travaillant dans des secteurs sensibles. Même si ses objectifs demeurent inconnus à ce jour, il semblerait que FLAME rechercherait en particulier les fichiers de type AutoCAD, qui sont utilisés pour les dessins industriels, les plans d'architecte, etc.

Compte tenu de la complexité de FLAME, et même s'il est très difficile d'identifier son auteur, les spécialistes considèrent qu'un tel virus n'a pu être conçu que par un Etat et de forts soupçons pèsent sur les Etats-Unis.

Pour Eugène Kaspersky, fondateur de la société éponyme, *« FLAME représente une nouvelle étape dans la cyberguerre »*. D'après lui, *« il faut bien comprendre que de telles armes peuvent être facilement utilisées contre n'importe quel pays. Et contrairement à la guerre conventionnelle, les pays les plus développés sont ici les plus vulnérables »*.

B. LA FRANCE N'EST PAS ÉPARGNÉE PAR CE FLÉAU

Le Livre blanc sur la défense et la sécurité nationale de 2008 avait mis l'accent sur le risque d'une attaque informatique de grande ampleur en France dans les quinze prochaines années, d'origine étatique ou non, laissant présager un potentiel très élevé d'atteintes à la vie courante, de paralysie de réseaux critiques pour la vie de la Nation, ou de déni de fonctionnement de certaines capacités militaires.

Aujourd'hui, on peut avoir le sentiment que le principal risque porte moins sur une attaque informatique massive visant à perturber les fonctions vitales du pays, que sur **l'espionnage informatique**, qui est un phénomène moins visible mais tout aussi inquiétant. En effet, avec l'espionnage informatique, notre pays, comme d'autres pays dans le monde, est menacé par un « pillage » systématique de son patrimoine diplomatique, culturel, scientifique et économique.

Comme cela a été confirmé à votre rapporteur par les représentants des organismes publics chargés de la sécurité des systèmes d'information, les administrations françaises, les entreprises ou les opérateurs font aujourd'hui l'objet **de manière quotidienne** de **plusieurs millions de tentatives d'intrusion dans les systèmes d'information**.

Si la plupart de ces attaques informatiques sont détectées et arrêtées avant de parvenir à pénétrer dans les systèmes, grâce aux mesures de protection mises en place, comme les anti-virus ou les pare-feux, il arrive que certaines d'entre-elles parviennent à contourner les mesures de protection et échappent à la vigilance des responsables de la sécurité informatique.

Ces dernières années, de nombreux organismes, publics ou privés, ont ainsi été victimes dans notre pays d'attaques informatiques, à l'image du ministère des affaires étrangères, du ministère de la défense ou encore du Commissariat à l'énergie atomique.

Comme le note le document préparatoire à l'actualisation du Livre blanc, *« les attaques informatiques contre les systèmes d'information des Etats et des entreprises, et plus particulièrement de celles qui appartiennent à des secteurs d'activité stratégiques, se sont multipliées. Ces attaques portent atteinte aux données sensibles (technologiques, commerciales, scientifiques, etc.) de leurs cibles. Elles sont souvent de* ***grande ampleur****, résultant d'une* ***longue préparation*** *et d'un* ***ciblage précis****. Elles peuvent nécessiter, pour leur mise en œuvre, des moyens dont* ***seul un Etat*** *ou* ***une organisation importante*** *et déterminée sont capables de disposer »*.

Votre rapporteur a choisi d'illustrer les menaces pesant sur notre pays au travers de trois exemples d'attaques informatiques, de nature et aux objectifs très différents.

1. La perturbation de sites institutionnels : l'exemple du Sénat

Peu avant l'adoption par le Parlement français, le 31 janvier dernier, de la loi visant à réprimer la contestation des génocides reconnus par la loi, dont le génocide arménien[1], de nombreux sites institutionnels, à l'image du site Internet de l'Assemblée nationale ou les sites de plusieurs députés, ont été rendus inaccessibles à la suite d'attaques informatiques. Votre rapporteur a pensé utile de décrire l'attaque subie à cette occasion par la Haute assemblée.

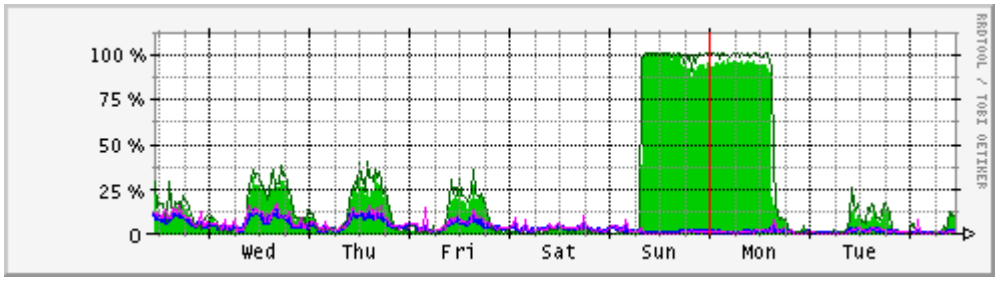
Le dimanche 25 décembre, le service informatique du Sénat a, en effet, été alerté par plusieurs fonctionnaires qui s'étaient rendus compte que le site Internet de la Haute assemblée n'était plus accessible. Dès le lendemain matin, les informaticiens ont constaté que le Sénat avait été victime de ce que les spécialistes appellent une « attaque par déni de service ». Par des moyens techniques, et notamment grâce à une copie du site Internet du Sénat sur un

[1] *cette loi a été déclarée contraire à la Constitution par le Conseil constitutionnel dans sa décision du 28 février 2012*

autre serveur, d'une capacité de résistance supérieure, il a été possible de rendre le site Internet de la Haute assemblée à nouveau accessible dès le lundi 26 décembre après midi.

A l'image du cas de l'Estonie en 2007, ces « attaques par déni de service » (*Denial of service – DOS*) visent à **saturer un ordinateur ou un système en réseau sur internet** en dirigeant vers lui un volume considérable de requêtes. On parle également de déni de service distribué (*Distributed denial of service – DDOS*) pour des attaques fonctionnant sur le même principe, mais dont l'effet est démultiplié par l'utilisation d'ordinateurs compromis et détournés à l'insu de leurs propriétaires. La masse de requêtes qui parvient simultanément sur un même système dépassant ses capacités, celui-ci n'est plus en mesure de fonctionner normalement. La paralysie d'un système d'information par ce type d'attaques est relativement facile à obtenir lorsqu'il s'agit d'un service accessible au public sur le réseau internet, à l'image du site Internet du Sénat.

Dans le cas du Sénat, l'attaque informatique, assez rudimentaire, et ayant mobilisé un nombre relativement faible d'ordinateurs, a eu pour effet de saturer, par un nombre très élevé de requêtes, l'accès au site Internet de la Haute assemblée pendant plusieurs heures.



Comme on peut le voir sur le graphique ci-dessus, qui représente la bande passante du réseau Internet du Sénat, la saturation a brutalement commencé peu après 6 heures du matin le dimanche 25 décembre et s'est achevée le lundi 26 décembre après midi.

Même si ces attaques informatiques ont été ouvertement revendiquées par des groupes de « hackers » patriotiques turcs, à l'image des groupes *« GrayHatz »* et *« Millikuvvetler »*, et par d'autres *« hackers »* indépendants, il est très difficile d'identifier précisément l'auteur de ces attaques.

En effet, ces groupes ont recours à des *« botnets »*, c'est-à-dire à des réseaux de machines compromises et utilisées à l'insu de leurs propriétaires.

Dans le cas du Sénat, la provenance des attaques informatiques ayant abouti à la saturation du site Internet était très diversifiée puisqu'elles provenaient d'ordinateurs situés partout dans le monde.

Si, depuis cette affaire, des mesures ont été prises au Sénat afin de renforcer la protection des systèmes, il n'en demeure pas moins que les attaques par déni de service visant un site Internet ouvert au public sont très difficiles à éviter et qu'il n'existe pas de parade absolue.

2. L'attaque informatique ayant visé le ministère de l'économie et des finances

Fin décembre 2010, alors que la France vient de prendre la présidence du G8 et du G20, les services du ministère de l'économie et des finances sont alertés par leurs correspondants étrangers de manifestations anormales dans leurs systèmes d'information.

En effet, dans la nuit du 30 au 31 décembre 2010, puis dans la nuit du 31 décembre au 1er janvier 2011, des courriels contenant une pièce jointe piégée semblant provenir d'interlocuteurs habituels de la direction du Trésor arrivent à destination de leurs correspondants étrangers du G20, qui découvrent ces pièces jointes et en alertent immédiatement leurs collègues français.

Le ministère de l'économie et des finances décide alors de saisir l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui envoie une trentaine de ses agents dans les locaux de Bercy.

Pendant près de deux mois environ, les équipes de l'ANSSI et de Bercy s'efforcent de pendre la mesure de la situation : Que se passe-t-il exactement ? Sommes-nous en présence d'une attaque informatique causée par un programme malveillant et de quel type ? Combien et quels sont les ordinateurs infectés ?

Cette première phase s'effectue dans la plus grande discrétion car, afin de prendre la mesure exacte de l'ampleur de l'attaque informatique, il est nécessaire de surveiller les mouvements de l'attaquant sans éveiller ses soupçons.

Au cours de cette première phase, il est apparu que **le ministère de l'économie et des finances avait été victime d'une intrusion informatique** menée à l'aide d'outils d'attaques informatiques**, principalement des logiciels espions**, introduits par le biais d'un ***« cheval de Troie »*.**

Les **logiciels espions** sont généralement déposés sur les postes des utilisateurs par le biais de ***« chevaux de Troie »*** prenant la forme de pièces jointes ou de pages web piégées, d'apparence inoffensives, souvent personnalisées pour contourner la vigilance de l'utilisateur. Une fois installés, ces programmes malveillants ouvrent une ***« porte dérobée »*** sur l'ordinateur infecté permettant aux attaquants de se connecter à distance sur les postes infectés pour y intercepter des frappes claviers et des communications réseaux et surtout procéder à des exfiltrations de documents sensibles vers des serveurs distants. La sophistication de certains de ces programmes permet de fractionner les exfiltrations, afin de les rendre moins détectables dans le flux normal de communication. Enfin, il est possible, à partir d'un ordinateur d'infecter d'autres ordinateurs, voire de prendre le contrôle de la totalité du système, en se dotant des prérogatives d'un « super administrateur » du réseau.

Si des logiciels espions peuvent être utilisés dans le cadre d'attaques d'ampleur réalisées à des fins de fraude bancaire, dans le cas de Bercy, les attaques découvertes semblent similaires à des attaques pour lesquelles les soupçons s'étaient portés sur la Chine. Comme cela est souvent le cas avec ce type d'attaques ciblées, les logiciels espions utilisés n'ont pas été détectés par les nombreux anti-virus du marché mais auraient pu l'être si des dispositifs de surveillance spécifiques avaient été déployés.

Par ailleurs, un certain nombre d'utilisateurs étaient dotés du statut d'« administrateur » de leurs postes de travail et pouvaient ainsi installer librement des applications. Les équipements de sécurité, notamment la passerelle d'accès à Internet, n'étaient pas correctement configurés et les *« journaux d'évènements »* (les *« logs »*) qu'ils génèrent n'étaient pas vérifiés. Le responsable informatique ne disposait d'aucune cartographie générale du réseau et il a fallu plusieurs semaines pour identifier toutes les passerelles vers l'Internet.

Lors de cette **première phase d'analyse**, environ 150 ordinateurs infectés ont été identifiés, principalement au sein de la direction générale du Trésor et de l'administration centrale, ce qui représente un pourcentage relativement faible au regard des 170 000 ordinateurs que compte le ministère. En revanche, aucune activité suspecte n'a été découverte sur les systèmes d'autres directions, comme la direction générale des finances publiques par exemple. Si aucune donnée à caractère personnel n'a été collectée, il y a de fortes probabilités pour que des documents relatifs notamment à la présidence française du G8 et du G20 aient été dérobés et exfiltrés.

Par ailleurs, si cette attaque a été découverte au début de l'année 2011 et que la direction générale du Trésor, direction du ministère en charge de la présidence française du G8 et du G20 était principalement visée, il semblerait, d'après plusieurs articles de presse, que l'origine de cette attaque informatique soit bien antérieure, certains journalistes ayant évoqué une durée de plusieurs semaines, voire plusieurs mois.

En tout état de cause, cette attaque a été qualifiée de *« première attaque contre l'Etat français de cette ampleur et à cette échelle »* par le directeur général de l'ANSSI, M. Patrick Pailloux.

Comme il l'a indiqué, sans toutefois citer nommément un pays, ces attaques sont l'œuvre de professionnels *« qui ont agi avec des moyens importants nécessitant préparation et méthode »*.

Si la caractéristique de ces techniques d'intrusion est leur **furtivité**, qui les rend difficilement décelables grâce à des outils de dissimulation de leur activité (*rootkits*) et qu'il est toujours difficile d'identifier précisément la provenance de ces attaques, de forts soupçons se portent, toujours d'après la presse, vers la Chine[1].

[1] *Voir à cet égard l'article paru dans le magazine « Paris Match », du 7 mars 2011*

En effet, certains indices peuvent laisser penser que des agences officielles, ou du moins des officines chinoises, sont à l'origine de ces attaques. Le ministère des finances du Canada avait lui-aussi été victime d'une attaque informatique en 2010 dans le cadre de sa présidence du G20, et les autorités canadiennes avaient publiquement mis en cause la responsabilité de la Chine dans ces attaques.

Ce n'est d'ailleurs pas la première fois que la Chine est soupçonnée d'être à l'origine d'intrusions informatiques sur des sites gouvernementaux à des fins d'espionnage, comme en témoignent les attaques informatiques dont ont été victimes plusieurs pays occidentaux au cours des années 2006 et 2007, attaques qualifiées à l'époque par la presse d'« attaques chinoises », qui avaient notamment visé en France le ministère des affaires étrangères ou le Commissariat à l'énergie atomique.

A l'époque, les autorités françaises avaient indiqué que ces attaques avaient transité par la Chine, tout en restant prudentes sur leur origine exacte qui n'avait pas pu être établie. En effet, si les serveurs ayant contrôlé les attaques étaient localisés en Chine, on ne peut exclure qu'ils aient simplement servi de relais. La particularité de ces attaques est en effet de procéder par rebonds, en utilisant une succession d'adresses intermédiaires pour mieux en dissimuler l'origine.

Plus récemment, d'après un article du *Washington Post*, plus de 70 organisations, dont l'ONU, auraient été victimes d'espionnage informatique et, là encore, la presse a évoqué une probable responsabilité de la Chine.

Au total, la première phase du traitement de l'attaque informatique contre Bercy, qui a duré environ deux mois, a permis d'analyser les codes malveillants et de déterminer l'ensemble des mesures à mettre en œuvre.

Lors d'une **deuxième phase**, menée lors du week-end des 5-6 mars 2011, afin de ne pas perturber le fonctionnement du ministère, et sous couvert d'une opération de maintenance informatique, l'ensemble des systèmes et réseaux informatiques du ministère ont été interrompus, dans le cadre d'une vaste opération de reconstruction et d'assainissement des systèmes, qui a concerné environ 12 000 postes de travail et qui s'est prolongée pendant environ six semaines. L'ensemble des ordinateurs infectés ont été remplacés et des mesures ont été mises en place afin d'assurer une meilleure protection des systèmes d'information.

Au cours d'un entretien particulièrement intéressant avec le Secrétaire général de Bercy, votre rapporteur a pu mieux mesurer l'importance du rôle de l'ANSSI et des efforts réalisés par le ministère de l'économie et des finances pour faire face aux conséquences de cette attaque informatique.

Depuis cette affaire et grâce à l'implication de son Secrétaire général, le ministère de l'économie et des finances a mis en œuvre un plan très complet de sécurisation de son système d'information sur un périmètre beaucoup plus large que celui qui avait été visé par l'attaque.

Ce plan s'inspire très fortement des recommandations de l'ANSSI et sa mise en œuvre fait l'objet d'un suivi attentif au niveau des directions. Vis-à-vis des agents, la principale difficulté a été de leur faire accepter les mesures de restriction relatives aux accès Internet. Par exemple, alors qu'il existait auparavant une liste « noire » de sites Internet dont la consultation était interdite, elle a été remplacée par une liste « blanche » contenant les seuls sites Internet dont l'accès est autorisé. Parallèlement, l'accès à *Twitter* a été supprimé.

Selon les dernières informations recueillies par votre rapporteur, parmi les 500 recommandations de l'ANSSI, les recommandations prioritaires de l'ANSSI ont été mises en œuvre tandis que le déploiement des autres s'applique progressivement sur les 170 000 postes de travail.

Cependant, une grande vigilance reste de mise. Comme l'a souligné le Secrétaire général du ministère de l'économie et des finances, M. Dominique Lamiot lors d'un entretien avec votre rapporteur : *« Fort classiquement, plus on s'éloigne dans le temps d'une crise, plus la tentation de desserrer les contraintes de sécurité s'accroît. C'est en cela qu'il est de notre responsabilité de trouver le bon équilibre entre sécurité et qualité de service aux utilisateurs »*.

Enfin, votre rapporteur regrette que, malgré la présence au sein du ministère de l'économie et des finances de nombreux corps d'inspection, aucune enquête interne n'ait été diligentée à la suite de cette affaire pour déterminer d'éventuelles responsabilités et qu'aucune évaluation n'ait été faite du préjudice politique, diplomatique et financier de cette attaque.

3. L'espionnage via l'Internet des entreprises : le cas d'AREVA

Comme l'ont confirmé à votre rapporteur les représentants des administrations publiques en charge de la sécurité des systèmes d'information, **les entreprises françaises sont aujourd'hui massivement victimes d'attaques informatiques non détectées**, qui visent notamment à capturer des informations portant sur leurs dirigeants, leurs clients et leurs fournisseurs, leurs technologies ou encore leurs contrats ou leurs stratégies, notamment à l'export.

S'il n'existe pas de données chiffrées, tout laisse à penser que **le préjudice subi par ces entreprises, et par voie de conséquence, sur l'économie française dans son ensemble, est considérable**, tant en termes financiers et de parts de marchés, que d'emplois.

Certains indices, tels que le mode opératoire et les techniques utilisées, les secteurs d'activité auxquelles appartiennent les entreprises visées, laissent à penser que certaines attaques relèvent d'une **stratégie ciblée**, qui ne peut être l'œuvre que d'organisations structurées, voire de services étatiques étrangers, à l'image de services de renseignements.

A cet égard, l'attaque informatique subie par le groupe AREVA, qui a été révélée par la presse, offre une bonne illustration des risques liés à l'espionnage informatique des entreprises.

Le 29 septembre 2011, le magazine *L'Expansion* a révélé, en effet, que **le groupe nucléaire français AREVA avait été victime d'une attaque informatique de très grande ampleur**[1].

Selon cet article, *« ces intrusions n'étaient pas nouvelles. Elles dureraient depuis deux ans et ne toucheraient pas seulement la France, mais aussi les sites étrangers d'AREVA »*. Il est indiqué que *« des hackers auraient, durant ces deux dernières années, réussi à pénétrer le réseau informatique du groupe et à prendre le contrôle d'ordinateurs »*. L'article évoque aussi *« des préjudices sur le plan stratégique, ce qui pourrait signifier le vol de secrets industriels »*. Enfin, l'auteur évoque dans son article *« une origine asiatique »*.

A la suite de la révélation de cette affaire, votre rapporteur s'est longuement entretenu avec les représentants du groupe AREVA. Ceux-ci ont présenté à votre rapporteur la manière dont cette attaque a été découverte et les mesures mises en place, avec l'aide de l'ANSSI, pour y faire face et renforcer la protection des systèmes d'information du groupe.

Comme cela arrive fréquemment dans ce type d'affaires, l'attaque a été décelée à partir d'un incident informatique relativement mineur – un « signal faible » disent les spécialistes – un informaticien ayant signalé un mouvement inhabituel et étrange sur le réseau de gestion.

La direction de l'entreprise a immédiatement saisi l'ANSSI et la direction centrale du renseignement intérieur, qui ont envoyé des équipes à la direction des systèmes d'information du groupe.

La forte implication personnelle des dirigeants du groupe a permis d'établir une relation de confiance et de confidentialité avec l'Etat et de manifester une forte volonté et autorité en matière de rétablissement des systèmes et de mesures de protection. En revanche, afin de ne pas éveiller les soupçons des attaquants et mettre en difficulté l'entreprise, il a été décidé de ne pas rendre publique cette intrusion.

La gestion de cette crise a ensuite suivi, à l'image de l'affaire de Bercy, une procédure en plusieurs étapes.

Dans **une première phase**, les équipes se sont attachées à analyser les caractéristiques de l'attaque et le comportement de l'attaquant. Ils ont ensuite repéré les machines infectées et ont préparé un plan de défense destiné à l'éradication de l'attaque et la reconstruction des composants affectés du système d'information.

Comme dans le cas de l'attaque informatique subie par le ministère de l'économie et des finances, il est apparu qu'AREVA avait été victime d'une

---

[1] *Charles Haquet, « Areva victime d'une attaque informatique de grande ampleur », publié dans « L'Expansion », le 29 septembre 2011*

intrusion informatique, menée grâce à un *« cheval de Troie »*, qui a permis aux attaquants d'accéder à des composants de type bureautique du système d'information.

En revanche, les systèmes industriels pilotant les activités sensibles des installations nucléaires n'ont pas été affectés, étant par ailleurs totalement isolés par conception et construction.

Lors d'une **deuxième phase**, minutieusement préparée, les équipes d'AREVA, de l'ANSSI et de prestataires privés ont procédé à un vaste plan d'assainissement de l'ensemble des systèmes d'information du groupe.

Au cours de cette phase simultanée à une opération de maintenance planifiée, il a été procédé à la mise en œuvre d'un plan de renforcement de la sécurité des systèmes.

Dans les semaines qui ont suivi, des mesures de sécurité complémentaires de même nature que celles recommandées à Bercy ont été apportées. Elles ont entraîné une modification des habitudes des utilisateurs, mais la direction informatique du groupe, soutenue par sa hiérarchie, a su imposer les choix nécessaires.

Au total, le coût pour l'entreprise de cette opération d'assainissement et de reconfiguration d'une partie de son système d'information a été de l'ordre de plusieurs millions d'euros, sans prendre en compte le préjudice économique éventuel résultant du vol des informations.

Lors de leur entretien avec votre rapporteur, les représentants d'AREVA ont rendu hommage aux très grandes compétences professionnelles de l'ANSSI et à la qualité de leur collaboration.

C. UNE MENACE PROTÉIFORME

La menace représentée par les attaques contre les systèmes d'information se caractérise par sa très grande diversité, qu'il s'agisse des techniques utilisées, des cibles visées ou de leurs auteurs présumés.

1. Les principaux types d'attaques informatiques

Dans son rapport d'information, notre ancien collègue M. Roger Romani distingue **trois modes principaux de « guerre informatique »** :

- **la « guerre par l'information »**, qui utilise le vecteur informatique dans un but de propagande, de désinformation ou d'action politique ;

- **la « guerre pour l'information »**, qui vise à pénétrer les réseaux en vue de récupérer les informations qui y circulent ou y sont stockées ;

- **la « guerre contre l'information »**, qui s'attaque à l'intégrité de systèmes informatiques pour en perturber ou en interrompre le fonctionnement.

On peut également classer les différents types d'attaques contre les systèmes d'information en **trois catégories** selon **leurs objectifs** :

- les attaques visant à **déstabiliser** des particuliers, des entreprises ou des Etats, par la perturbation de sites Internet ou encore par l'altération ou la révélation de données obtenues via les systèmes d'information ;

- les attaques ayant pour objectif d'**espionner** des particuliers, des entreprises ou des Etats afin de s'approprier leurs ressources ;

- les attaques visant à **saboter** ou à **détruire** des ressources informatiques ou des équipements matériels.

Les attaques de saturation par déni de service, le vol ou l'altération de données grâce à un logiciel malveillant et la destruction d'un système par un virus informatique constituent trois types d'attaques informatiques largement utilisées aujourd'hui.

● ***Les attaques par déni de service***

Les attaques par déni de service (*Denial of service – DOS*) visent à **saturer un ordinateur ou un système en réseau sur internet** en dirigeant vers lui un volume considérable de requêtes.

L'agresseur peut n'utiliser qu'un seul ordinateur, mais ce cas de figure est rare en pratique. Le plus souvent, il fera appel à un nombre important d'ordinateurs compromis, réunis dans un réseau de « zombies » (« botnets »). On parle alors de « déni de service distribué » (*Distributed denial of service – DDOS*) pour des attaques fonctionnant sur le même principe, mais dont l'effet est démultiplié par l'utilisation d'ordinateurs compromis et détournés à l'insu de leurs propriétaires. Les évènements d'Estonie en 2007 en constituent l'exemple type. La masse de requêtes qui parvient simultanément sur un même système dépassant ses capacités, celui-ci n'est plus en mesure de fonctionner normalement.

Les « ***botnets*** » désignent les réseaux de machines compromises (ou machines « zombies ») qui sont aux mains d'individus ou de groupes malveillants (les « maîtres ») et leur permettent de transmettre des ordres à tout ou partie des machines et de les actionner à leur guise.

Le « *botnet* » est constitué de **machines infectées par un virus informatique** contracté lors de la navigation sur internet, lors de la lecture d'un courrier électronique (notamment les *spams*) ou lors du téléchargement de logiciels. Ce virus a pour effet de placer la machine, à l'insu de son propriétaire, aux ordres de l'individu ou du groupe situé à la tête du réseau. On estime aujourd'hui que le **nombre de machines infectées** passées sous le contrôle de pirates informatiques est considérable. Il pourrait atteindre le quart des ordinateurs connectés à l'internet, soit environ 150 millions de machines.

Le **détenteur du réseau est rarement le commanditaire de l'attaque**. Il monnaye sa capacité d'envoi massive à des « clients » animés de préoccupations diverses. La constitution de tels réseaux est ainsi utilisée en

vue de l'envoi de courriers électroniques non désirés (*spams*) à des fins publicitaires ou frauduleuses, ou encore afin de dérober des informations personnelles de la cible visée. L'attaque par déni de service n'est qu'une des applications possibles. Son corollaire est le chantage au déni de service, c'est-à-dire l'extorsion de fonds auprès des entreprises ou organismes en échange d'une levée des attaques de saturation.

La paralysie d'un système d'information par ce type d'attaques est relativement facile à obtenir lorsqu'il s'agit d'un service accessible au public sur le réseau Internet. Comme le relève la note d'information de l'ANSSI consacrée à ce sujet, *« la lutte contre les dénis de service est souvent une affaire de rapport de forces et, à défaut de pouvoir les empêcher, la victime potentielle peut prendre des dispositions pour en atténuer les effets sur ses processus »*[1].

La vulnérabilité des réseaux internes, en principe non accessibles de l'extérieur, est moindre, mais elle est liée au degré d'étanchéité entre ces réseaux et l'Internet.

Or les systèmes d'information internes sont de plus en plus ouverts pour répondre aux besoins de mobilité des personnels et de communication avec des partenaires extérieurs.

● ***Le vol ou l'altération de données***

Le vol ou l'altération de données contenues sur des réseaux informatiques peuvent être réalisés par des moyens variés.

Les plus simples reposent sur l'intervention humaine, soit par intrusion, soit par le jeu de complicités internes, soit par le vol d'équipements (notamment les ordinateurs portables). Les plus sophistiqués font appel à des techniques d'écoute des flux d'information ou d'interception des rayonnements émis par les équipements et qualifiés, dans cette hypothèse, de « signaux compromettants ».

S'agissant des **intrusions sur les systèmes d'information par des voies informatiques**, l'une des techniques utilisées est celle du « **cheval de Troie** », c'est-à-dire d'un programme informatique ou d'un fichier comportant une fonctionnalité cachée connue de l'attaquant seul et lui permettant de prendre le contrôle de l'ordinateur compromis, puis de s'en servir à l'insu de son propriétaire. Un « cheval de Troie » se cache en général dans un programme d'aspect inoffensif ou usuel, et son activation implique l'intervention de l'utilisateur (ouverture d'une pièce jointe, utilisation d'un lien de connexion à un site internet). A la différence des virus propagés à une très grande échelle, les « chevaux de Troie » constituent le plus souvent des attaques ciblées, adaptées à la victime choisie, qui ne peuvent être détectées automatiquement par les antivirus. Ils s'installent durablement sur la machine compromise. Cette technique peut être utilisée pour intégrer l'ordinateur visé dans un réseau de machines compromises (*botnet*).

---

[1] *Note d'information du CERTA, « Dénis de service – Prévention et réaction », 27 janvier 2012*

Elle couvre aussi les différents modes d'intrusion ayant pour but d'**accéder aux informations contenues dans l'ordinateur**, voire de les modifier. Peuvent ainsi être installés des programmes enregistrant la frappe de l'utilisateur sur le clavier (« *keylogger* ») en vue de récupérer des données confidentielles (mots de passe, coordonnées bancaires) et le contenu des fichiers créés, ainsi que des **logiciels espions** (« *spyware* ») permettant de transmettre à des tiers des informations sur les usages habituels des utilisateurs du système, par exemple ses données de connexion. Il est également possible par ce biais de transférer vers un ordinateur extérieur les fichiers stockés dans l'ordinateur compromis. La sophistication de ces programmes permet de fractionner ces envois afin de les rendre moins détectables dans le flux normal de communication. Enfin, il est possible par ce biais de s'introduire dans d'autres ordinateurs utilisant le même réseau, voire de prendre le contrôle de l'ensemble du réseau en usurpant les droits des administrateurs.

La caractéristique de ces techniques d'intrusion est leur **furtivité**, qui les rend difficilement décelables, grâce à des outils de dissimulation d'activité (*rootkits*).

Il est à noter que l'installation de tels programmes malveillants peut aussi bien s'effectuer par d'autres moyens, par exemple le branchement par la personne visée d'un périphérique (clef USB, assistant personnel) qui aura été préalablement infecté. De ce point de vue, **l'usage de plus en plus répandu d'équipements mobiles (comme des ordinateurs portables, des ordiphones ou des tablettes) ou d'ordinateurs personnels pour un usage professionnel constituent des risques supplémentaires pour l'intégrité des réseaux**. Leur connexion à un réseau interne après avoir été infectés à l'extérieur rend inopérants les dispositifs de sécurité tels que les pare-feux.

Enfin, l'**externalisation de certains traitements informatiques** représente un risque potentiel dès lors que les précautions nécessaires ne sont pas prises vis-à-vis des sous-traitants quant à la protection de données sensibles, notamment pour les services gouvernementaux.

Ainsi, le ***« Cloud computing »*** (ou « informatique en nuage »), qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur, ce qui permet aux utilisateurs ou aux entreprises de délocaliser et de mutualiser la gestion de leur système informatique, présente des **risques majeurs** du point de vue de la sécurité informatique.

● ***Les attaques visant à détruire***

Certaines attaques informatiques visent à perturber gravement voire à détruire les systèmes d'information. On parle ainsi parfois de véritables « armes informatiques ».

C'est notamment le cas de STUXNET qui est parvenu à causer des dégâts assez considérables en détruisant notamment des centrifugeuses utilisées pour l'enrichissement de l'uranium en Iran.

● ***Les différentes vulnérabilités***

Les attaques informatiques exploitent généralement des vulnérabilités ou des failles contenues dans les systèmes d'information.

De manière schématique, on peut distinguer trois types de vulnérabilités :

- les vulnérabilités qui tiennent à **la conception même des systèmes ou aux défauts de réalisation** : le défaut de conception résulte du choix initial du concepteur et peut difficilement être corrigé alors, que le défaut de réalisation résulte de la fabrication (mauvais codage par exemple) et peut être atténué par des opérations correctrices ;

- les **failles liées à l'organisation ou à l'environnement** : il s'agit de vulnérabilités liées aux mauvaises conditions d'emploi, qu'il s'agisse de leur processus d'emploi (le paramétrage par exemple) ou de leur environnement. Elles peuvent être diminuées ou supprimées de différentes façons ;

- les **vulnérabilités qui résultent de l'usage fait par les utilisateurs** : elles tiennent notamment au non respect des mesures de sécurité associées à l'exploitation d'un produit. Ces failles peuvent être corrigées mais cela nécessite une sensibilisation particulière des utilisateurs.

Il convient de noter qu'il existe un véritable **marché privé d'échange de vulnérabilités** de certains logiciels ou systèmes. Ainsi, en 2011, environ 7000 failles ont été publiées sur Internet.

Par ailleurs, on peut aisément trouver sur Internet des logiciels malveillants prêts à l'emploi. 26 millions de codes malveillants auraient ainsi été créés l'an dernier et diffusés sur Internet[1].

2. Les cibles visées

Les attaques informatiques peuvent aussi bien viser des particuliers que des entreprises ou des institutions publiques. En ce qui concerne celles mettant en cause la défense ou la sécurité nationale, les **services de l'Etat**, les **opérateurs d'importance vitale** et les **entreprises intervenant dans des domaines stratégiques ou sensibles** sont particulièrement concernés.

Toutefois, ces attaques n'emportent pas le même type de conséquences selon qu'elles visent des sites ou services accessibles au public, des systèmes opérationnels ou plus directement des personnes détentrices d'informations sensibles.

● ***Les sites et services accessibles au public***

On pourrait penser que l'attaque de leurs sites Internet ne met pas directement en cause le fonctionnement même de l'Etat, des services publics ou des entreprises.

[1] *Rapport annuel 2012 de PandaLabs*

Provoquer l'indisponibilité du site Internet d'une institution ou d'une administration, comme on l'a vu en Estonie ou en France lors de la discussion de la loi réprimant la négation du génocide arménien, répond essentiellement à un objectif politique, de même que la défiguration (*defacement*) du contenu et son remplacement par des messages à connotation protestataire ou revendicative. Pour une entreprise, le préjudice s'évaluera davantage en termes d'image, avec d'éventuelles incidences commerciales.

Cependant, un très grand nombre de ces sites abritent également des **services en ligne** qui se sont considérablement développés ces dernières années et dont l'**interruption** causerait d'**importantes perturbations dans la vie sociale et économique de la nation**.

On pense ici aux relations des particuliers avec l'administration de l'Etat ou les collectivités territoriales, qui ont mis en place de nombreuses possibilités de démarches en ligne, ou avec des entreprises commerciales (entreprises de transport, services financiers, commerce par internet), ainsi qu'aux relations entre les entreprises elles-mêmes (relations avec les fournisseurs et les sous-traitants).

Compte tenu de la place prise aujourd'hui par ces services, leur indisponibilité produirait un effet de désorganisation et entraînerait de sérieuses pertes économiques.

On peut également mentionner l'utilisation croissante d'équipements informatiques ou de systèmes d'information par les différentes administrations, comme par exemple le « bracelet électronique » pour le ministère de la justice ou la vidéosurveillance par les polices municipales, la police nationale et la gendarmerie nationale.

● ***Les systèmes opérationnels : le cas des opérateurs d'importance vitale et des systèmes d'information militaires***

Les réseaux internes des administrations et des entreprises sont a priori moins vulnérables aux attaques extérieures, dès lors qu'ils sont indépendants des sites internet accessibles au grand public. Toutefois, rares sont désormais les organisations qui utilisent pour leurs activités opérationnelles (gestion administrative et financière, processus industriels) des applications développées spécifiquement et totalement isolées du réseau extérieur. Pour des raisons de coût et de simplicité, le recours à des applications disponibles sur le marché est privilégié. Par ailleurs, la densification des échanges d'information ou encore les procédés de gestion à distance et de télémaintenance vont à l'encontre du principe de cloisonnement censé protéger ces systèmes des agressions extérieures.

Une attention particulière doit être portée sur les **installations d'importance vitale** (réseaux de transport, de distribution d'eau et d'électricité). Celles-ci utilisent des **systèmes de supervision et de régulation** communément désignés par leur acronyme anglais **SCADA** (*Supervisory, control and data acquisition*), qui permettent de surveiller et contrôler sur une

aire géographique très étendue des opérations telles que la gestion de l'électricité ou de l'eau, la signalisation des feux ou les flux de transport. Grâce à ces systèmes, les opérateurs peuvent agir à distance sur des automates industriels ou des commandes.

Si de tels systèmes étaient le plus souvent particulièrement sécurisés par leur rusticité technique et leur indépendance des autres réseaux, ils font désormais plus largement appel à des technologies modernes appliquant les protocoles internet standard, pour des raisons économiques, mais aussi parce qu'elles sont souvent les seules disponibles sur le marché. Les vulnérabilités potentielles de ces produits à large diffusion sont particulièrement analysées et exploitées par les pirates informatiques.

Ainsi, le ver *Conficker* a eu en 2009 des répercussions sur des appareils médicaux partout dans le monde et notamment en France alors même qu'il ne contenait aucun code malveillant.

Enfin, s'agissant des installations d'importance vitale, il faut signaler qu'une évolution majeure est en cours avec la **convergence des réseaux téléphoniques et internet**. La généralisation de la « voix sur IP » rendra les communications téléphoniques vulnérables aux mêmes types d'attaques que les systèmes informatiques.

Votre rapporteur souhaite également mentionner la question spécifique des **capacités militaires**.

Les **systèmes d'information opérationnelle et de commandement**, utilisés dans les systèmes d'armes, les transmissions de données et les communications militaires, sont généralement isolés des autres réseaux. Toutefois, le nombre croissant de systèmes utilisés et leur interconnexion avec une multitude de terminaux, conformément au principe des opérations en réseaux, élargit le périmètre d'éventuels points de vulnérabilité. L'utilisation d'applications informatiques disponibles sur le marché « grand public » augmente elle aussi les risques de vulnérabilité.

Ainsi, en 2011, un virus informatique aurait ainsi infecté les postes de commande à distance des drones américains *Predator* et *Reaper* effectuant des missions en Afghanistan et sur d'autres théâtres. Le virus aurait été introduit dans les ordinateurs de la base américaine via des disques durs externes. Un drone américain aurait aussi été détourné au-dessus de l'Iran en décembre 2011. D'après l'université du Texas, le détournement d'un drone au moyen d'un leurre ou du brouillage du signal civil du GPS serait réalisable pour un coût d'environ 1000 dollars et il serait ensuite relativement aisé de transformer ce drone en missile.

● ***Les détenteurs d'informations sensibles***

Les détenteurs d'informations sensibles, au sein de l'appareil d'Etat, des grandes institutions de recherche ou des entreprises, y compris petites ou moyennes, constituent un troisième type de cibles potentielles pour des attaques informatiques.

On se situe ici dans le champ des **activités d'espionnage ou d'ingérence**, au travers de **méthodes nouvelles, notamment des logiciels espions introduits grâce à des « chevaux de Troie »** visant à cibler les ordinateurs et les systèmes mobiles ou périphériques de personnes identifiées en fonction de leur niveau de responsabilité et de leurs contacts.

Le recours aux technologies d'intrusion peut intervenir en complément ou à la place d'autres modes de captation de données informatiques, telles que le vol d'ordinateurs portables des personnes cibles ou leur « fouille » informatique, par exemple aux passages de frontières.

L'objectif est d'acquérir des informations d'intérêt politique, diplomatique, militaire, économique, scientifique, technologique ou industriel.

3. Le profil des « attaquants » : pirates informatiques, cybercriminels, cyberterroristes, Etats étrangers ?

L'**identification de l'origine d'une attaque informatique est particulièrement difficile**. Les procédés utilisés font le plus souvent appel à une succession d'ordinateurs pouvant être situés dans plusieurs pays. Remonter la chaîne des machines impliquées supposerait des enquêtes extrêmement longues, tributaires des aléas de la coopération judiciaire internationale. Les méthodes de dissimulation sont nombreuses et vont du détournement d'ordinateurs à l'insu de leur propriétaire au recours à des ordinateurs publics et anonymes, comme ceux situés dans les cybercafés.

Malgré tout, la plupart des services gouvernementaux et des observateurs désignent, derrière ces attaques, des groupes de pirates informatiques dont les méthodes semblent de plus en plus sophistiquées.

● ***Les « pirates » informatiques : un profil qui se « professionnalise »***

L'image plutôt sympathique du « pirate informatique » a été notamment popularisée auprès du grand public par le personnage de Lisbeth Salander, dans la trilogie policière *« Millennium »* du suédois Stieg Larsson.

A l'évidence, les attaques informatiques actuelles ne peuvent être imputées à de simples « amateurs » isolés, procédant par jeu ou par défi et désireux de tester ou de démontrer leur niveau de performance technique.

Avec l'essor de l'internet s'est développée une **nouvelle catégorie de pirates informatiques** (*hackers*), qui agissent individuellement ou en groupes.

On peut distinguer trois catégories de « hackers » selon leurs motivations :

- Les **« chapeaux blancs »** *(« white hats »)* : Il s'agit souvent de consultants en sécurité informatique, d'administrateurs réseaux ou de cyberpoliciers, qui se caractérisent par leur sens de l'éthique et de la déontologie ;

- Les **« chapeaux gris »** *(« grey hats »)* pénètrent dans les systèmes sans y être autorisés, pour faire la preuve de leur habileté ou pour alerter l'organisme visé des vulnérabilités de ses systèmes, mais ils ne sont pas animés par des intentions malveillantes ou criminelles ;

- Enfin, les **« chapeaux noirs »** *(« black hats »)* regroupent les cybercriminels, les cyberespions ou les cyberterroristes. Ce sont eux qui répandent volontairement les virus informatiques. Ils sont essentiellement motivés par l'appât du gain. Ces individus ou ces groupes mettent au point des outils qu'ils peuvent exploiter directement ou offrir sur le marché à des clients tels que des organisations criminelles ou mafieuses, des officines d'espionnage économique, des entreprises ou des services de renseignement.

L'attaque par déni de service reste le mode opératoire privilégié de ces groupes qui semblent toutefois également maîtriser des technologies plus complexes et plus discrètes de pénétration des systèmes d'information pour y dérober des données.

Les « pirates informatiques » peuvent également être subdivisés en fonction de leurs spécialités. Ainsi, le *« craker »*, s'occupe de casser la protection des logiciels, le *« carder »* les systèmes de protection des cartes à puces, le *« phreaker »* les protections des systèmes téléphoniques.

● ***Les groupes de « hackers patriotiques »***

Les « pirates informatiques » peuvent parfois agir de leur propre initiative par motivation « patriotique ». Cette hypothèse a été avancée lors de la crise diplomatique russo-estonienne du printemps 2007, ainsi que pour diverses attaques informatiques par exemple entre Israël et l'Arabie Saoudite.

La presse a fait état de l'existence de tels groupes en Russie et dans des pays de l'ex-Union soviétique, où leurs activités ne seraient guère entravées.

Nombre de pirates informatiques agiraient également depuis la Chine. Ont notamment été cités la « *Red Hacker's Alliance* » qui, selon la presse de Taïwan, compterait près de 20 000 membres, le groupe « *Titan Rain* », le groupe *« Hack4.com »* ou encore la « *China Eagle Union* ».

● ***Le « hacktivisme » : nouvelle forme de contestation sociale ?***

L'un des groupes les plus importants de « hackers » est toutefois la mouvance *Anonymous*, qui compterait plusieurs milliers de membres. Les personnes se revendiquant de ce groupe apparaissent en public le visage dissimulé par le masque de Guy Fawkes, ce révolutionnaire anglais du XVIe siècle qui a inspiré le masque porté par le personnage de « V » dans la bande dessinée *« V pour Vendetta »* et son adaptation au cinéma.

L'emblème du groupe Anonymous

Les membres qui se revendiquent de cette mouvance dénoncent ce qu'ils considèrent comme des atteintes à la liberté d'expression sur l'Internet et prétendent défendre un « Internet libre et ouvert à tous ».

Anonymous avait déjà lancé en 2008 des attaques informatiques contre l'église de scientologie, puis lors des manifestations en Iran, mais ce groupe s'est surtout fait connaître en 2010, grâce à une opération dénommée *« Operation Payback »*, par des attaques informatiques coordonnées contre les adversaires de la contrefaçon de musique et de vidéo sur Internet. Il a également apporté son soutien aux manifestants lors du « printemps arabe » et à la diffusion, par *Wikileaks*, d'environ 250 000 télégrammes diplomatiques confidentiels américains.

Plus récemment, après l'annonce en janvier 2012 par le FBI de la fermeture du site de partage *MegaUpload, Anonymous* a lancé des attaques informatiques contre de nombreux serveurs gouvernementaux américains, tels que le FBI ou le département de la justice. En France, le site de la présidence de la République, qui avait approuvé par un communiqué la fermeture de *Megaupload*, ainsi que ceux du ministère de l'Intérieur, de Hadopi ou de *L'Express* ont également été visés. Le groupe aurait également mis en ligne les données personnelles de plusieurs dizaines de policiers.

En France, il existe d'autres groupes de « pirates informatiques », comme « telecomix.com » qui défend la liberté d'expression sur Internet.

● ***La cybercriminalité***

Qu'il s'agisse de l'escroquerie sur Internet, de la contrefaçon illégale, de la fraude à la carte bancaire ou encore de la pédopornographie sur Internet, il est banal de constater aujourd'hui la place préoccupante prise par la cybercriminalité, à mesure de l'utilisation croissante des nouvelles technologies. Le coût global du cyber crime a été estimé en 2011 à 209 milliards de dollars[1].

[1] *Symantec, Norton Cybercrime Report 2011, september 2011*

Et, comme le relève M. Nicolas Arpagian dans son livre consacré à la cybersécurité : *« l'éloignement géographique ou la langue ne sont pas sur la Toile des protections efficaces ni des immunités durables »*[1].

S'il n'entrait pas dans le cadre de la mission confiée à votre rapporteur de traiter ces aspects, qui relèvent davantage des services de police et de gendarmerie et de la justice, l'importance prise par la cybercriminalité, l'implication de véritables organisations criminelles et ses effets potentiellement déstabilisateurs sur l'ensemble de l'économie peuvent faire de cette menace un risque majeur pour la Nation et justifient donc une action résolue de la part de la puissance publique pour renforcer les moyens de lutte contre ce fléau.

Cela passe notamment par une meilleure sensibilisation des entreprises et des consommateurs, le renforcement des moyens dévolus aux services spécialisés de la police, de la gendarmerie et des douanes, ainsi que de ceux de la justice, par une meilleure coopération internationale, le partenariat avec le secteur privé et le développement de produits sécurisés.

● ***Le risque de « cyberterrorisme »***

L'utilisation de l'arme informatique par des groupes terroristes, soit directement, soit indirectement par l'intermédiaire de pirates informatiques qu'ils rémunèreraient, est un risque qui a été fréquemment évoqué.

Les groupes terroristes utilisent largement Internet à des fins de propagande et de prosélytisme, ainsi que comme moyen de communication, y compris semble-t-il aux moyens de systèmes de chiffrement. En revanche, **aucune attaque terroriste d'envergure par voie informatique**, par exemple contre des infrastructures sensibles, **n'a pour l'instant été répertoriée**.

On sait cependant que les organisations terroristes ont acquis une maîtrise significative des outils informatiques et de l'Internet qui pourrait leur permettre de mener des attaques plus sérieuses. A titre d'exemple, la branche armée du Jihad islamique palestinien a déclaré avoir mis en place une unité de « cyberguerre » qui revendique des attaques contre des sites militaires et des sites de journaux israéliens. Par ailleurs, les groupes de pirates restent susceptibles de monnayer leurs services auprès de ces organisations.

● ***Vers une « cyberguerre » ?***

Peut-on parler de « cyberguerre » et imaginer que les attaques informatiques se substitueront aux modes d'action militaires traditionnels et que l'issue des conflits se jouera à l'avenir sur ce nouveau champ de bataille ?

Il s'agit sans doute d'une hypothèse assez extrême[2].

---

[1] *Nicolas Arpagian, "La cybersécurité", Que-sais-je ?, août 2010, p.20*

[2] *Voir à ce sujet l'article de J. Arquilla et D. Ronfeldt « cyberwar is coming ! » de 1993, le livre de Richard A. Clarke et Robert K. Knake « Cyberwar », HarperCollins Publishers, ou encore l'article de M. Thomas Rid, « La cyberguerre est un mythe »*

Il semble acquis en revanche que l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information. C'est par exemple ce qui s'est passé lors du conflit entre la Russie et la Géorgie en août 2008.

Ainsi, pour M. Daniel Ventre[1], comme pour M. Olivier Kempf[2], le cyberespace constitue un nouveau milieu, qui se superpose aux milieux traditionnels (terre, mer, air), à l'espace et au nucléaire, ce qui n'implique pas pour autant qu'il domine les autres ou que la « cyberguerre » constitue à elle seule un milieu autonome de la guerre.

Ce nouveau facteur nécessite toutefois des stratégies et des modes d'action très spécifiques.

Voilà un vaste champ de réflexion qui s'ouvre pour la pensée stratégique, par ailleurs d'une remarquable qualité, au sein de nos forces armées et, plus largement, dans le monde de la défense !

● ***Etats-Unis, Chine, Russie : une probable implication des Etats ?***

Si nombre de pays, à l'image des Etats-Unis, reconnaissant ouvertement développer des capacités offensives dans le domaine informatique, aucune attaque informatique n'a jusqu'à présent été publiquement revendiquée par un Etat.

Même dans le cas de STUXNET, où les forts soupçons pesant sur les Etats-Unis et Israël ont été confirmés par les révélations du journaliste David E. Sanger, et plus encore dans le cas de FLAME, les autorités américaines se sont bien gardées d'admettre leur responsabilité.

De même, alors que de nombreux indices peuvent laisser penser à une implication de la Russie dans les attaques informatiques ayant visé l'Estonie en 2007 ou la Géorgie à l'été 2008, les autorités de Moscou n'ont jamais admis être à l'origine de ces attaques.

De nombreux documents officiels américains pointent également du doigt la responsabilité première de la Chine, en particulier dans le domaine de l'espionnage informatique.

Ainsi, dans un rapport du Pentagone sur la montée en puissance de la Chine de mai 2012, on peut lire que *« la Chine a largement recours à l'espionnage industriel à des fins militaires, qui implique aussi bien les services de renseignement que les instituts de recherche et les sociétés*

---

[1] Voir les ouvrages de M. Daniel Ventre « Cyberattaque et cyberdéfense » et « Cyberespace et acteurs du Cyberconflit » ainsi que le livre dirigé par M. Daniel Ventre « Cyberguerre et guerre de l'information – stratégies, règles et enjeux » aux éditions Lavoisier.

[2] Voir notamment l'ouvrage co-dirigé par Stéphane Dossé et Olivier Kempf "Stratégie dans le cyberspace", Esprit du Livre, 2011

privées » et que *« les acteurs chinois sont les responsables les plus actifs et les plus obstinés au monde dans le domaine de l'espionnage économique »* [1].

On peut aussi mentionner l'« opération Aurora »[2] ayant visé, entre fin 2010 et début 2011, les comptes Gmail de plusieurs défenseurs chinois des droits de l'homme aux Etats-Unis, en Europe et en Asie.

Les autorités de Pékin ont toujours démenti ces accusations en mettant en avant le fait que **la Chine serait elle aussi une victime**.

Ainsi, lors d'un séminaire intitulé *« Cybersécurité : la Chine et le monde »*, qui s'est tenu en mai dernier à Pékin, en présence de plus de 80 experts originaires d'une vingtaine de pays, le chef adjoint de l'état major de l'armée populaire de libération chinoise, le général Ma Xiaotian, a rappelé que la Chine était également victime d'un grand nombre d'attaques informatiques et il a appelé la communauté internationale à conjuguer ses efforts pour formuler des règles contraignantes afin de réguler le « cyberespace ».

La Chine, qui est le pays qui compte le plus d'internautes au monde, figurerait ainsi à la première place des pays victimes d'attaques informatiques, avec 217 millions d'utilisateurs chinois d'Internet victimes en 2011, selon un rapport du CERT national chinois publié en mars 2012.

---

[1] *Department of Defense, Annual Report to Congress, "Military and Security Developments involving the People's Republic of China 2012", May 2012.*

[2] *« Google China cyberattack part of vast espionnage campaign, experts say » par Ariana Eunjung et Ellen Nakashima, The Washington Post, 14 janvier 2010*

II. UNE MENACE DÉSORMAIS PRISE EN COMPTE AU NIVEAU INTERNATIONAL

Les attaques contre les systèmes d'information s'affranchissent des frontières et peuvent être dirigées simultanément contre plusieurs Etats. La surveillance des réseaux et la mise au point des réactions en cas d'incident justifie une coopération et une assistance internationales. De manière plus générale, la protection des systèmes d'information face aux activités illégales constitue aujourd'hui une préoccupation commune à de nombreux Etats et à plusieurs organisations internationales. Toutefois, la coopération internationale dans ce domaine se heurte encore à de nombreux obstacles.

A. UNE PRÉOCCUPATION PARTAGÉE PAR NOS PRINCIPAUX ALLIÉS

Les Etats-Unis, le Royaume-Uni et l'Allemagne ont fait depuis déjà plusieurs années de la cybersécurité une priorité nationale et ont mis en place des dispositifs importants pour lutter contre les attaques informatiques.

1. Les Etats-Unis

Héritage d'une attention portée de longue date au renseignement d'origine technique et à la protection de l'information, ainsi que d'efforts accentués sur ces problématiques durant la Guerre Froide, les Etats-Unis accordent **une priorité stratégique à la protection des systèmes d'information.**

Les Etats-Unis sont, en effet, l'un des pays qui dépend le plus d'Internet et qui subit le plus d'attaques informatiques au monde. A titre d'exemple, au niveau gouvernemental, les systèmes du département de la défense, le Pentagone, et ceux des forces armées regroupent 15 000 réseaux et 2 millions d'utilisateurs. Le *« cybercommander »*, le général Keith B. Alexander, a indiqué récemment que ces systèmes étaient attaqués près de six millions de fois par jour. Au cours des dernières années, des intrusions informatiques graves dans les systèmes d'information du Pentagone, du département d'Etat, du département de la sécurité intérieure ou encore de la NASA ont été constatées. Ainsi que cela a été récemment rendu public, en 2008, le réseau informatique du *Central Command*, le commandement stratégique régional américain pour le Moyen-Orient basé à Tampa en Floride, a été infecté à l'aide d'une clé USB, aboutissant à la compromission de réseaux et d'informations classifiés.

En mai 1998, signe d'une prise en compte précoce de la problématique de la cybersécurité, le Président Bill Clinton a signé le décret présidentiel 63 sur la protection des infrastructures critiques visant à notamment éliminer les vulnérabilités de leurs systèmes informatiques au regard d'attaques cybernétiques comme physiques.

En janvier 2008, le Président George W. Bush a approuvé la *Presidential National Security directive 54* qui formalise une série de mesures visant à protéger les systèmes d'information gouvernementaux contre les attaques informatiques.

Enfin, **le Président Barack Obama s'est fortement investi sur le sujet et a fait de la cybersécurité l'une des priorités de son mandat.** Ainsi, dans un discours du 29 mai 2009, il a déclaré que *« la menace cybernétique est l'un des plus importants défis auxquels doivent faire face les Etats-Unis, en matière économique et au regard de la sécurité nationale »* et que *« la prospérité de l'Amérique au XXIe siècle dépendra de la cybersécurité »*[1]. Il a nommé en décembre 2009 à la Maison Blanche un conseiller spécialement chargé de ce dossier, rendant compte aussi bien au Conseil pour la sécurité nationale qu'à l'équipe en charge des questions économiques, M. Howard Schmidt, qui vient de quitter ses fonctions[2] et dont l'une des principales missions a été d'unifier la doctrine nationale américaine et d'améliorer la coordination inter-agences sur ce dossier. Son service a publié en mai 2011 *« une stratégie internationale pour le cyberespace »*[3].

La cybersécurité a de fait pris une place croissante dans la stratégie de défense et de sécurité nationale américaine. Elle figure ainsi au nombre des premières priorités de la stratégie de sécurité nationale, publiée en 2010[4], qui considère que la cybersécurité est l'un des principaux défis qui pèse sur la sécurité nationale, la sécurité publique et l'économie. *« Quand on me demande ce qui m'empêche de dormir la nuit. Je réponds : la cybermenace »* déclarait en janvier 2010 le Secrétaire adjoint à la défense, M. William J. Lynn III.

En juillet 2011, le Pentagone a publié **une nouvelle stratégie cybernétique** (surnommée « Cyber 3.0 ») [5], qui fait suite à plusieurs rapports[6]. Le document est centré sur la *« défense active »*, à savoir renforcer les mesures traditionnelles de protection du réseau par d'autres capacités, s'appuyant par exemple sur le renseignement électronique. Cette nouvelle stratégie souligne par ailleurs l'importance d'une coopération plus étroite à la fois au niveau national, entre les différentes agences et entre le secteur public et le secteur privé, que sur le plan international.

Elle contient cinq axes :

- un effort en matière d'organisation, d'entraînement et de formation et d'équipements de manière à ce que le département de la défense traite le cyberespace comme un domaine opérationnel et puisse tirer tous les avantages du potentiel qu'il offre ;

---

[1] *« Remarks by the President on securing our nation's cyberinfrastructure", 29 mai 2009*
[2] *M. Howard Schmidt a annoncé sa démission le 17 mai 2012, celle-ci prenant effet fin mai.*
[3] *The White House, « International Strategy for Cyberspace : Prosperity, Security and Openness in a Networked World », Washington, mai 2011.*
[4] National Security Strategy*, 2010*
[5] *Department of Defense, "Strategy for Operating in Cyberspace", Juillet 2011*
[6] dont la *Quadriennal Defense Review*

- l'emploi de nouveaux systèmes de défense pour protéger les réseaux et systèmes informatiques du département de la défense ;

- le partenariat avec les autres agences et le secteur privé ;

- des relations solides avec les alliés et les partenaires internationaux ;

- l'augmentation de l'expertise en matière cyber et des innovations technologiques.

L'ambition américaine est non seulement d'assurer une protection efficace des systèmes d'information mais de garantir la supériorité des Etats-Unis dans le cyberespace.

Comme votre rapporteur l'a constaté lors de son déplacement à Washington, il existe **de nombreux organismes** qui interviennent aux Etats-Unis en matière de cybersécurité.

Le département de la sécurité intérieure (*Department of Homeland Security - (DHS)*, créé après les attaques du 11 septembre 2001 afin de regrouper diverses agences compétentes en matière de sécurité du territoire national, couvre le domaine de la protection des infrastructures critiques, notamment les réseaux de communication.

Au sein du DHS, la *National Cyber Security Division* (NCSD), créée en juin 2003, est chargée plus spécialement de la cybersécurité. Une unité de la NCSD, l'US-CERT[1], sorte de « bras armé » de la NCSD, est chargée de la protection des infrastructures Internet nationales et de la coordination de la réponse aux cyberattaques à leur encontre, ainsi que dans les réseaux de l'administration fédérale.

Le FBI, au travers de ses équipes d'actions cybernétiques, CATS (*Cyber Action Teams*), est quant à lui chargé d'enquêter sur les affaires de cybercriminalité portant atteinte aux intérêts nationaux, et notamment de lutter contre les intrusions informatiques affectant les entreprises américaines importantes. Ses équipes sont ainsi venues en aide à Google, en mai 2011, afin d'enquêter sur le piratage des comptes officiels Gmail du gouvernement.

Le département de la défense joue également un rôle important.

S'agissant des **capacités techniques**, elles sont détenues par la *National security agency (NSA)*, agence du renseignement technique en charge des actions défensives (surveillance et réaction) au sein du département de la défense et offensives (écoute et intrusion) dans le domaine des systèmes d'information. L'*Information assurance directorate* assure au sein de la NSA l'expertise sur les questions de cryptographie et de protection des systèmes d'information et compte environ **3 000 agents**. Cette direction, qui contribue par ailleurs à traiter les incidents opérationnels, est l'homologue de l'ANSSI.

En mai 2010, un *« cybercommand »* interarmées (USCYBERCOM) a été créé afin de renforcer la coordination entre les différentes armées et de

[1] *United States Computer Emergency Readiness Team*

donner un cadre aux actions offensives menées à son compte par la NSA. Chaque armée dispose d'un centre cyber « propre » qui travaille au profit de Cybercommand (*24th Air Force, 10th Fleet, 2nd Army* et le *Marine Corps Forces Cyberforce Command*). Dirigé par le Général Keith B. Alexander, qui est dans le même temps directeur de la NSA, le *« cybercommand »* est chargé de *« planifier, coordonner, intégrer, synchroniser et conduire des opérations de défense des réseaux spécifiques du département de la défense, ainsi que de préparer et de conduire des opérations militaires dans le cyberespace afin d'assurer la liberté d'action américaine dans le cyberespace et d'empêcher à ces adversaires d'y agir »*. Il lui revient également la tâche primordiale de centraliser les différentes opérations cybernétiques afin de renforcer les compétences de la défense. Il est placé sous l'autorité de l'USSTRATCOM, le commandement des forces stratégiques des Etats-Unis.

De manière schématique, **les responsabilités se répartissent donc de la manière suivante :**

- La protection du territoire américain et des infrastructures « critiques » relève du DHS et du département de la justice ;

- Les aspects militaires de défense des infrastructures « critiques », de la base industrielle du soutien aux autorités civiles et des opérations militaires (c'est-à-dire le volet offensif) sont placés sous la responsabilité du département de la défense et du directeur du renseignement national ;

- La sécurité nationale des systèmes : c'est le département de la défense qui est chargé de ce volet ;

- Les enquêtes criminelles : le DHS et le département de la justice en sont responsables ;

- Le renseignement relève du département de la défense et du directeur du renseignement national.

On constate toutefois **des difficultés de coordination au sein et entre les départements de la défense et de la sécurité intérieure** et les nombreuses structures qui interviennent dans le domaine de la cyberdéfense.

Ainsi, lorsqu'en septembre 2010 le général Alexandre B. Keith souhaite élargir les compétences du *« cybercommand »* à la protection des infrastructures critiques, la Secrétaire générale du département de la sécurité nationale, Mme Janet Napolitano, lui répond dans un discours que l'effort de sécurisation des infrastructures critiques devrait être effectué par une agence civile, et non par le secteur militaire[1].

C'est la raison pour laquelle le 13 octobre 2010, un *memorandum of agreement* a été signé entre le département de la sécurité intérieure et le département de la défense qui prévoit une coordination interministérielle et un partage du personnel, de l'équipement et des infrastructures, afin de renforcer

---

[1] *Department of Homeland Security, « Remarks by Secretary Napolitano at the Atlantic's Cybersecurity Forum », 17/12/2010*

la cybersécurité. Cet accord fait également en sorte que les capacités de renseignement et les compétences techniques de la NSA servent en soutien des actions cybernétiques du DHS.

Pour autant, **la coordination ne semble pas encore optimale** entre ces différentes structures, ainsi qu'entre les agences de l'Etat et le secteur privé. En témoigne notamment cette affirmation entendue de la part de représentants de la NSA à propos du département de la sécurité intérieure : *« We have the know-how, they have the responsability »*, que l'on peut traduire par *« Nous détenons la compétence, mais ce sont eux qui ont la responsabilité officielle »*.

Les Etats-Unis procèdent à un **renforcement de leur organisation et de leurs moyens.**

Sur **le plan législatif**, **trois lois distinctes** simplifient les interventions de l'exécutif en cas de cyberattaques contre des infrastructures énergétiques critiques, tandis qu'un **autre texte de loi** assure la coordination des efforts accrus en matière de cybersécurité, dont ceux concernant les institutions financières et l'industrie[1].

On peut également mentionner :

- l'extension du programme EINSTEIN à toute l'administration et aux agences fédérales. Ce programme vise à déployer un **dispositif de surveillance permettant de détecter toute activité suspecte sur les réseaux**. Il est opérationnel depuis plusieurs années sur les réseaux du Département de la défense. La NSA, agence de renseignement technique américaine, est la cheville ouvrière de ce programme qui pourrait être étendu aux installations d'importance vitale.

- la réduction, de 2 000 à 50 du nombre de points d'accès des réseaux de l'administration à l'internet, en vue de faciliter le déploiement de dispositifs de sécurité et de surveillance ;

- le renforcement des dispositifs permettant de maîtriser l'acquisition des équipements dans le domaine de l'informatique et des communications électroniques qui sont importés aux Etats-Unis.

Les autorités américaines ont établi une liste de leurs **infrastructures critiques et de leurs ressources vitales** qu'il convient de protéger contre des cyberattaques[2]. Vingt-sept secteurs d'infrastructures critiques et de ressources clés ont été identifiées.

Ainsi, le 4 mai dernier, le département de la sécurité intérieure a mis en garde les services de santé contre les dangers liés à l'utilisation d'appareils

---

[1] *Cyber Security Enhancement Act Redux, Government Information Security Articles, 10 février 2011.*

[2] *Department of Homeland Security, "National Infrastructure Protection Plan, Partnering to enhance protection and resiliency", 2009.*

médicaux connectés à l'Internet[1]. Les défibrillateurs et les pompes à insuline pilotés à distance sont particulièrement en cause. Les autorités américaines rappellent également les dangers induits par la généralisation des tablettes et des ordiphones parmi le personnel soignant qui peuvent exposer les données médicales des patients.

Les autorités américaines ont également engagé depuis déjà plusieurs années **une étroite coopération avec le secteur privé.**

La *RSA Conférence* réunit ainsi tous les ans la plupart des acteurs, tant publics que privés, de la cybersécurité aux Etats-Unis.

Le Pentagone coopère étroitement avec les entreprises américaines du secteur de la défense, notamment Lockheed Martin, Northrop Grumman, Raytheon, General Dynamics, Boeing, mais aussi des sociétés de services, telles que SAIC, L3, Booz Allen, ainsi que Cisco et Symantec. En 2007, le département de la défense a lancé un programme de cybersécurité et de protection de l'information (CS/IA) de la base industrielle de défense. Ce programme, basé sur le volontariat, est destiné aux entreprises du secteur de la défense et consiste à échanger des informations techniques et opérationnelles sur les menaces. Il réunit actuellement une quarantaine d'entreprises et devrait être étendu à l'ensemble des sous-traitants du secteur de la défense. D'après les informations recueillies par votre rapporteur, ce programme a permis de mieux comprendre les attentes des entreprises, de renforcer la confiance et de mettre en place une collaboration étroite entre secteur public et secteur privé.

Le marché de la cybersécurité est évalué à 23 milliards de dollars aux Etats-Unis, soit près de la moitié du marché mondial, évalué de l'ordre de 50 milliards de dollars, dont environ la moitié (15 milliards de dollars) est constitué d'appels d'offres provenant du secteur public, du département de la sécurité nationale ou du département de la défense nationale. Le département de la sécurité nationale dispose d'un budget de l'ordre de 3 milliards de dollars pour la recherche et le développement en matière de cybersécurité.

On notera aussi que les Etats-Unis consacrent des moyens conséquents à la réalisation de simulations et d'exercices. Ainsi, le *Departement of Homeland Security* a réalisé à trois reprises, en février 2006, en mars 2008 et en septembre 2010, trois exercices de grande ampleur, baptisés *« CyberStorm I », « CyberStorm II »* et *« CyberStorm III »* simulant une attaque informatique visant notamment les infrastructures de communication, les transports et les systèmes bancaires. Impliquant une quarantaine d'entreprises du secteur privé ainsi que quatre pays étrangers (Australie, Canada, Nouvelle-Zélande, Royaume-Uni), l'exercice *« CyberStorm II »* était doté d'un budget supérieur à 6 millions de dollars. En 2012, le DHS a aussi organisé un exercice « cyber » de très grande ampleur (NLE 2012, *National Level Exercise*). Le but était d'examiner la capacité américaine à coordonner et répondre à une attaque cyber. Dix Etats américains

[1] *NCCIC du 04/05/2012*

étaient impliqués, le secteur privé et toutes les agences compétentes. L'Australie, le Canada, la Nouvelle Zélande et le Royaume-Uni ont également participé à cet exercice.

Au total, de 2010 à 2015, le gouvernement américain devrait consacrer 50 milliards de dollars à la cyberdéfense[1], soit environ **10 milliards de dollars par an, et plusieurs dizaines de milliers d'agents travaillent sur ces aspects**.

Dans le contexte probable de diminution du budget de la défense aux Etats-Unis sur les dix prochaines années, qui devrait concerner l'ensemble des composantes militaires, les responsables américains ont annoncé que seuls deux secteurs verraient leurs moyens préservés, voire même augmentés : le renseignement et les capacités cyber.

Enfin, on sait que l'**armée américaine** est dotée d'une **doctrine intégrant la lutte informatique défensive** comme la **lutte informatique offensive**.

Une telle doctrine se retrouve ainsi dans le rapport du département de la défense au Congrès de novembre 2011 consacré au cyberespace[2]. D'après ce document, *« le Président des Etats-Unis se réserve le droit de répondre par tous moyens, y compris par des capacités cybernétiques, à un acte hostile dans le cyberespace dirigée contre les Etats-Unis, ses alliés ou partenaires ou ses intérêts, telle qu'une attaque informatique dirigée contre le gouvernement, l'armée ou l'économie des Etats-Unis »*. Et, il est indiqué plus loin que *« le département de la défense a les capacités de conduire des opérations offensives dans le cyberespace pour défendre la Nation, ses alliés et ses intérêts »*.

Au total, en dehors de la très forte disproportion des effectifs et des moyens, on constate **d'importantes différences d'approches** entre le modèle américain et le modèle français.

Contrairement aux autorités françaises, les autorités américaines n'hésitent pas à reconnaître publiquement qu'elles sont victimes d'un nombre élevé d'attaques informatiques et elles n'hésitent pas à mettre en cause publiquement le rôle de la Chine. Surtout, elles affirment clairement qu'elles se réservent le droit de répondre par tout moyen, y compris par des capacités offensives, à une attaque informatique visant le gouvernement, l'armée ou l'économie américaine.

Ainsi, selon un rapport du chargé des affaires asiatiques du Pentagone, *« la Chine accélère sa montée en puissance dans le domaine de*

---

[1] *"On Cyber Warfare", Paul Cornish, David Livingstone, Dave Clemente et Claire York, Chatham House Report, novembre 2010*

[2] *Department of Defense Cyberspace Policy Report, " A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011, Section 934, november 2011*

l'espionnage informatique utilisé comme un moyen d'intelligence économique, notamment au détriment d'entreprises américaines »[1].

La publication de ce rapport est intervenue peu après la rencontre des deux ministres de la défense des Etats-Unis et de Chine, MM. Leon Panetta et Liang Guanglie début mai. Les deux responsables ont posé les bases d'une coopération entre les deux pays dans le domaine de la sécurité des systèmes d'information.

Enfin, il existe une coopération entre les Etats-Unis et la France en matière de cybersécurité, qui nécessiterait toutefois d'être développée.

2. Le Royaume-Uni

Le Royaume-Uni est considéré, avec les Etats-Unis, comme l'un des pays ayant compris très tôt les enjeux de la cybersécurité et l'importance d'assurer la protection des systèmes d'information. Déjà, sous le précédent gouvernement travailliste de M. Gordon Brown, la stratégie de sécurité nationale de mars 2008 avait identifié les attaques contre les systèmes d'information comme une menace pour la sécurité du pays.

Le Premier ministre conservateur M. David Cameron a également fait de la cybersécurité **une priorité de son gouvernement**.

Le Royaume-Uni a fait l'objet de plusieurs cyberattaques, visant notamment le Foreign office, à l'été 2011, ainsi que le ministère de la défense, qui aurait subi un millier de cyberattaques en 2010, soit le double de l'année précédente. L'ancien ministre de la défense M. Liam Fox a déclaré en juin 2011 : *« Une bataille incessante est menée contre nous, jour après jour », « nos systèmes sont pris pour cible par des criminels, des services de renseignement étrangers et d'autres personnes malveillantes qui veulent espionner notre personnel, endommager notre système et voler des informations ». « Il n'y a pas de ligne Maginot dans le cyberespace. Notre propriété intellectuelle nationale dans le secteur des industries de défense et de sécurité est à la merci de pillage systématique »*[2].

La nouvelle stratégie du Royaume-Uni en matière de cybersécurité, qui a été publiée en novembre 2011[3], témoigne de l'engagement des autorités britanniques sur ce sujet.

Malgré un contexte budgétaire difficile, le Premier ministre britannique M. David Cameron a annoncé fin 2010 un effort supplémentaire de 650 millions de livres, soit **750 millions d'euros**, pour la cybersécurité sur les quatre prochaines années.

---

[1] *Departement of Defense, mai 2012, BBC News du 08/05/2012, AFP du 18/05/2012*
[2] Le Figaro, *8 décembre 2011*
[3] "The UK Cyber Security Strategy : Protecting and promoting the UK in a digital world", *November 2011*

Ces chiffres peuvent laisser songeur lorsque l'on sait que le budget de l'agence française chargée de la sécurité des systèmes d'information, l'ANSSI, est de l'ordre de **75** millions d'euros en 2012.

Comme votre rapporteur a pu le constater lors de ses entretiens à Londres, le Royaume-Uni a mis en place une organisation qui se caractérise par le fait qu'elle est rattachée directement aux services du Premier ministre (*cabinet office*). La stratégie britannique met également l'accent sur **la coopération entre le secteur public et les acteurs privés.**

L'architecture institutionnelle britannique actuelle en matière de cyberdéfense remonte pour l'essentiel à 2009, date à laquelle le gouvernement travailliste a adopté une stratégie nationale de cybersécurité. Cette stratégie a été revue dans le cadre de l'adoption de la *« Strategic defence and security review »* en octobre 2011, qui a adopté un *« transformative national cyber security programme »*.

Cette architecture est placée sous l'autorité de l'*« Office of cyber security and information assurance »* du Cabinet Office (services du Premier ministre), en charge de la coordination interministérielle globale, de l'élaboration de la stratégie du gouvernement, de la gestion des dépenses liées à la protection de la sécurité des systèmes d'information et de la supervision des relations avec le secteur privé et le public.

Le *Government Communications Headquarters* (GCHQ), agence en charge du renseignement technique (service de renseignement électronique du gouvernement britannique), est l'autorité technique nationale pour la protection des systèmes d'information (« information assurance ») et pour la cybersécurité. En dehors de son rôle d'agence de renseignement, elle assure donc des fonctions équivalentes à celles de l'ANSSI. Le GCHQ est chargé de conseiller et d'assister le gouvernement et les entités du secteur privé qui font appel à ses services sur la sécurité des communications et des données électroniques.

Historiquement, la responsabilité en matière de protection des systèmes d'information était portée par une sous-entité dédiée du GCHQ, le *Communications and Electronic security group* (CESG). Un cloisonnement existait entre le CESG et le reste du GCHQ. En 2011, le GCHQ a entamé une profonde mutation – la plus profonde depuis sa création aux dires des britanniques – puisque, pour mieux faire face aux enjeux de la cybersécurité, il a été décidé de faire tomber le cloisonnement entre le CESG et le reste du GCHQ. Le CESG n'est désormais plus qu'une image de marque pour les personnes affectées aux questions de protection des systèmes d'information.

En 2008, le CESG comptait 450 agents. Actuellement, on estime que **700 agents** travaillent au sein de cette agence sur les questions de cyberdéfense. Rappelons, qu'en France, l'ANSSI devrait compter 350 personnes fin 2013, après le renforcement décidé par le précédent gouvernement.

Le *cyber security operations center* (CSOC), créé en 2010 et hébergé par le GCHQ, a pour objectif de détecter en temps réel d'éventuelles cyber attaques, d'identifier leur provenance et les moyens d'y répondre. Après avoir été créé comme une structure autonome, le CSOC fait désormais partie intégrante du GCHQ.

D'autres départements ministériels se sont dotés de services spécialisés sur les différents aspects de la politique cybersécurité :

- le ministère de l'Intérieur (*Home Office*) et l'office de lutte contre la criminalité organisée (*Serious ans organised Crime Agency*) qui sont responsables de la lutte contre la cybercriminalité et le terrorisme sur Internet ;

- le ministère de la défense, notamment pour les « capacités offensives » ;

- ou encore le *Department for business innovation and skills* (BIS) qui a en charge les aspects relatifs aux télécommunications à la régulation et à la gouvernance de l'Internet.

Le *Centre for the protection of National Infrastructure* (CPNI), dont la mission consiste, au travers d'une approche partenariale, à s'assurer que les infrastructures sont sécurisées à bon niveau, traite désormais aussi le volet cybersécurité.

En novembre 2011, le gouvernement britannique a présenté **une nouvelle stratégie en matière de sécurité des systèmes d'information**.

Cette stratégie comprend quatre objectifs :

- lutter contre la cybercriminalité et faire du Royaume-Uni l'un des pays les plus sûrs en ce qui concerne le commerce dans le cyberespace ;

- renforcer la résilience contre les cyberattaques et mieux protéger les intérêts du Royaume-Uni dans le cyberespace ;

- conserver un cyberespace libre, ouvert et sécurisé pour le grand public ;

- renforcer la connaissance, les compétences et les capacités du Royaume-Uni en matière de protection et de sécurité des systèmes d'information.

Parmi les nombreuses mesures envisagées, on mentionnera en particulier :

- la poursuite du renforcement des capacités de l'agence chargée de la protection des systèmes d'information (GCHQ) et du ministère de la défense pour détecter et lutter contre les attaques informatiques ;

- l'établissement d'un partenariat avec le secteur privé pour le partage d'information sur les menaces du cyberespace ;

- le soutien aux entreprises et aux infrastructures critiques pour les inciter à renforcer la protection de leurs systèmes d'information ;

- le développement de la formation et le partage des connaissances ;

- la promotion d'un secteur industriel dense et innovant dans le domaine de la cybersécurité, et le renforcement de la coopération entre l'agence britannique et les entreprises.

La stratégie britannique met ainsi nettement l'accent sur **les relations avec le secteur privé.**

Dans le cadre de sa mission, le GCHQ développe une documentation technique sur la sécurité des systèmes d'information. Il ne semble pas exister à ce stade de directives ou d'instructions sur la déclaration des incidents mais, selon les éléments recueillis par votre rapporteur, le gouvernement britannique réfléchirait actuellement aux moyens d'encourager le secteur privé à davantage déclarer les incidents (certaines entreprises échangent déjà des informations avec le gouvernement sur une base informelle).

Le gouvernement britannique s'est ainsi doté de points de contacts pour la déclaration d'incidents :

- pour les entités gouvernementales (à l'exception du ministère de la défense où les incidents sont gérés par le *« UK defense cyber operations group »*, une *« Computer emergency response team »* a été créée au sein du GCHQ, le GovCERT-UK ;

- pour les entités faisant partie du réseau des infrastructures critiques, une *« computer emergency response team »* a été instituée au sein du *« Centre for the protection of national infrastructure » (CPNI).*

La création d'un point de contact pour la déclaration d'incidents destiné au secteur privé serait actuellement à l'étude.

Cette réflexion s'inscrit dans le cadre des efforts du gouvernement pour développer ses relations avec le secteur privé, et notamment pour les sensibiliser davantage à la menace que représente la cybercriminalité. Il y a un an, le Premier ministre M. David Cameron a ainsi réuni les dirigeants d'entreprises appartenant à des secteurs d'activités d'importance vitale pour évoquer avec eux les questions liées aux cybermenaces.

Sur le plan de **la coopération internationale**, le Royaume Uni a organisé les 1 et 2 novembre 2011 une conférence internationale à Londres consacrée à la cyberdéfense, qui a rassemblé plus de 700 personnes, dont un grand nombre de représentants de 61 pays (Etats-Unis, Russie, Chine, etc.), des représentants d'organisations internationales (ONU, UE, OTAN) et des représentants de la société civile et de l'industrie.

Le ministre des affaires étrangères du Royaume-Uni, M. William Hague, s'est prononcé lors de cette conférence en faveur de la liberté sur Internet et s'est montré réticent à l'idée d'une régulation d'Internet. Le Premier ministre britannique a, pour sa part, mis en exergue la détermination du gouvernement britannique à combattre les cyberattaques et à renforcer ses capacités de cybersécurité en relation avec le secteur privé. Il a estimé le coût

des cyberattaques pour l'économie britannique à plus de 27 milliards de livres par an.

Enfin, **la coopération franco-britannique** est très dense et l'ANSSI entretient des relations régulières avec le GCHQ.

La cyberdéfense fait également partie des domaines de coopération mentionnés par les accords franco-britanniques en matière de défense de novembre 2010. La coopération entre la France et le Royaume en matière de cyberdéfense est considérée comme l'une des plus développée, avec l'Allemagne.

3. L'Allemagne

Pour les responsables allemands, les menaces pesant sur la sécurité des systèmes d'information ne cessent de s'accroître en Allemagne, tant en ce qui concerne la fréquence, la diversité et le nombre d'attaques informatiques. Leur impact sur l'économie allemande est évalué à 61,5 millions d'euros pour l'année 2010, en augmentation de 66 % par rapport à 2009.

Le gouvernement fédéral a adopté, en février 2011, une nouvelle *« stratégie en matière de cybersécurité pour l'Allemagne »*[1]. Le principal objectif de cette stratégie est de renforcer la résilience globale de l'Allemagne face à ces risques, en développant les instruments de coordination au sein du gouvernement, mais surtout les liens avec le secteur privé. Il s'agit ainsi de développer une culture de cybersécurité partagée au niveau national.

La coordination en matière de cybersécurité incombe en Allemagne au **ministère fédéral de l'Intérieur** (BMI), dont votre rapporteur a rencontré l'un des responsables lors d'un déplacement à Berlin.

Sa mise en œuvre s'appuie sur l'agence homologue de l'ANSSI, le *Bundesamt für Sicherheit in des Informationstechnik* (BSI), l'office fédéral de sécurité des systèmes d'informations, qui est rattaché au ministère fédéral de l'intérieur et situé à Bonn. Le BSI dispose de compétences techniques assez comparables à celles de l'ANSSI (sensibilisation, analyse des risques, veille et alerte, développement de produits de sécurité, normalisation). Les prérogatives du BSI sur les questions relatives à l'identité électronique sont néanmoins plus larges que celles de l'ANSSI et recouvrent celles de l'Agence nationale des titres sécurisés (ANTS).

Son rattachement au ministère fédéral de l'intérieur ne lui permet cependant pas de disposer d'une véritable autorité interministérielle à l'égard des autres ministères, à la différence de l'ANSSI, et il doit aussi composer avec les Länder en raison du caractère fédéral du pays. Le BSI entretient cependant des liens beaucoup plus étroits avec les opérateurs d'infrastructures critiques et les entreprises sensibles.

---

[1] *« Cyber-Sicherheitsstrategie für Deutschland »*

Le BSI bénéficie d'une augmentation régulière de son budget et de ses effectifs, qui s'élevaient à 340 agents en 2001 et atteignent actuellement environ **560 agents,** avec un **budget annuel de 80 millions d'euros**.

La nouvelle stratégie allemande en matière de cybersécurité a abouti à la création d'un centre national de lutte contre la cybermenace (*Cyber Abwehrzentrum*). Cette nouvelle structure, implantée à Bonn, est responsable de la coordination des activités en matière de protection et de défense contre les cyberattaques sous le pilotage du BSI et avec la participation directe de l'office de protection de la Constitution (BfV) et de l'office fédéral pour la protection des populations et l'assistance en cas de catastrophe (BBK). Participent également, en tant qu'organismes associés, l'office fédéral de la police criminelle (BKA), de la police fédérale (BPol), des douanes (ZKA) et des services de renseignement (BND), ainsi que l'armée (BW). Il s'agit moins d'une autorité supplémentaire que d'une plate forme de coordination et d'échange d'information.

Ainsi, cet organe, dont les compétences précises restent à déterminer, devrait assurer des fonctions de centre de situation (évaluation de la nature et de l'origine des attaques), de centre de coordination en cas de crise, et de conseil pour l'ensemble de l'administration publique.

Le BSI devrait toutefois conserver un rôle central. C'est l'organe qui dispose des compétences techniques pour apporter une réponse aux cyber-attaques, définir des normes et des standards en matière de sécurité informatique s'imposant à l'ensemble des administrations et procéder à des achats groupés. Le BSI dispose, en effet, d'un programme d'investissement en matière de recherche et développement en sécurité informatique.

Par ailleurs, un *« Conseil national de sécurité cybernétique »* (*Cybersicherheitsrat*) associant des représentants de la Chancellerie fédérale et des grands ministères (affaires étrangères, intérieur, défense, justice, économie, finances), des Länder et du monde économique, a été créé. Ce conseil a vocation à définir les politiques transversales du gouvernement fédéral pour la cyberdéfense et à renforcer la coopération entre le gouvernement fédéral, les Länder et les acteurs économiques.

Le **véritable point fort** de la nouvelle stratégie allemande, notamment par rapport à la France, porte aux yeux de votre rapporteur sur **le renforcement de la résilience des infrastructures critiques.**

La stratégie allemande prévoit, en effet, une structuration systématique des relations avec les autorités de régulations ou de surveillance des opérateurs d'infrastructures critiques, dans les secteurs comme les transports, l'électricité ou le secteur bancaire, et, sur une base volontaire, avec d'autres acteurs du secteur privé.

Le plan *« Kritis »* de renforcement de la protection des infrastructures critiques, adopté en 2007, contenait déjà un volet « cyberdéfense » confiant au

BSI le soin de développer des partenariats avec des entreprises volontaires, secteur par secteur.

La nouvelle stratégie prévoit plusieurs mesures afin de **renforcer la protection des infrastructures critiques** :

- un **point de contact unique** devrait être désigné par les différentes entreprises d'un secteur sensible concerné, afin de faciliter les échanges entre l'autorité de régulation et le secteur privé. Les principaux secteurs « critiques » identifiés sont les transports, l'approvisionnement en eau et en électricité, les matières dangereuses, les télécommunications, le secteur bancaire et les assurances ;

- les entreprises pourront bénéficier des conseils du BSI, qui est autorisé à émettre des **mises en garde**, le cas échéant publiques, concernant les failles et vulnérabilités de certains produits de l'industrie informatique ou des télécommunications ;

- une **déclaration obligatoire au BSI** en cas d'incident informatique important est prévue pour les entreprises ;

- le BSI voit **ses relations renforcées** avec toutes les autorités publiques responsables de la supervision, de la surveillance ou de la sûreté des secteurs jugés critiques, tant au niveau fédéral, qu'au niveau des Länder, pour s'assurer de leurs capacités de prise en compte des risques cyber dans leurs secteurs ;

- la possibilité d'attribuer au Conseil national de cybersécurité de véritables fonctions de surveillance transsectorielle sur les questions de cybersécurité.

Néanmoins, contrairement à la France, l'approche de l'administration allemande vis-à-vis des infrastructures critiques n'est pas unifiée. Ainsi, le BBK dispose d'une large liste d'infrastructures critiques. Le BSI possède sa propre liste d'infrastructures critiques, qui ne recoupe que partiellement celle du BBK.

Il faut aussi souligner qu'à la suite de la réunification et du transfert de la capitale à Berlin, l'Allemagne s'est dotée d'une **infrastructure de communication** entre administrations fédérales extrêmement fiable et hautement sécurisée (*Informationverbund Berlin Bonn – IVBB*), dont la France est encore privée. Cette infrastructure offre aussi des services unifiés (hébergement de sites web, serveurs de messagerie, etc.) pour l'administration fédérale. Le BSI est responsable de la sécurité de l'ensemble de ce système, qui ne dispose que de deux points d'interconnexion à l'Internet. Cette caractéristique a facilité le déploiement d'outils automatiques de surveillance des réseaux informatiques gouvernementaux, qui ont permis à l'Allemagne de disposer très tôt d'une **capacité de détection globale de l'administration fédérale**, alors que la France disposait dans ce domaine d'un retard certain. Grâce à ces outils, l'administration fédérale n'a fait l'objet, depuis 2005, d'aucune intrusion informatique connue.

Par ailleurs, comme le révèlent plusieurs documents transmis par le ministère de la défense au Bundestag[1], l'armée allemande reconnaît plus ou moins ouvertement disposer de ***« capacités offensives »*** de base pour *« mener des attaques informatiques dans des réseaux ennemis »*.

Toutefois, ce sujet reste une question sensible en Allemagne, en raison notamment de l'absence de cadre légal, des limitations de la loi fondamentale allemande ou encore des réticences de l'opinion publique.

Sur le plan de **la coopération internationale**, la nouvelle stratégie évoque le développement d'une politique étrangère en matière de cybersécurité, confiée au ministère des affaires étrangères. L'objectif serait de renforcer l'action de l'Union européenne, à travers le plan d'action en matière de protection des infrastructures critiques et le renforcement de l'agence européenne chargée de l'expertise en matière de sécurité des systèmes d'information (ENISA).

Au niveau international, l'Allemagne souhaite privilégier l'efficacité, en recommandant l'adoption de règles juridiquement non contraignantes, donc plus rapides à négocier et à mettre en œuvre, avec l'idée d'un « code de bonne conduite » international dans le domaine cyber.

Comme votre rapporteur a pu le constater lors de ses entretiens à Berlin, **l'Allemagne souhaiterait renforcer sa coopération avec la France dans ce domaine**.

Il existe déjà une coopération très étroite entre l'ANSSI et le BSI. Ainsi, un représentant de l'ANSSI a participé, en tant qu'observateur, au dernier exercice de gestion de crise « Lükex 2011 », dont le thème était centré sur la sécurité des systèmes d'information.

Lors du XIIe Conseil des ministres franco-allemand, qui s'est tenu le 5 février 2010, l'ancien Président de la République et la chancelière allemande ont décidé la mise en place d'une coopération entre la France et l'Allemagne en matière de cybersécurité, notamment en matière d'échange d'informations et de concertation des positions au sein des instances internationales. Mais cette coopération mériterait d'être renforcée et élargie à d'autres domaines.

Ainsi, il semble qu'il existe une réelle volonté partagée entre la France et l'Allemagne de lancer une véritable coopération industrielle dans le domaine des produits de sécurité informatique, et, plus largement, dans le secteur des technologies de l'information et de la communication, afin de ne pas dépendre uniquement de produits américains ou asiatiques.

Pour votre rapporteur, **la cyberdéfense pourrait ainsi constituer l'un des volets de la relance de la coopération franco-allemande**, notamment dans la perspective de la célébration du cinquantenaire du traité de l'Élysée en 2013.

---

[1] *Un rapport de la commission de la défense du Bundestag d'avril 2012 intitulé « Cyberwarfare » a ainsi été cité le Financial Times Deutschland*

B. UNE COOPÉRATION INTERNATIONALE ENCORE BALBUTIANTE

Plusieurs organisations multilatérales ont mis la sécurité des systèmes d'information à l'ordre du jour de leurs travaux.

En particulier, ce thème fait aujourd'hui l'objet de nombreux débats au sein de l'OTAN et de l'Union européenne.

1. Des initiatives en ordre dispersé

Assez curieusement, **la Chine et la Russie sont aujourd'hui les principaux promoteurs de règles contraignantes au niveau international sur la sécurité dans le cyberespace.** Ainsi, ces deux pays ont proposé en 2009 un code de conduite à l'Assemblée générale des Nations Unies[1]. La Russie a également proposé une résolution sur la sécurité de l'information en vue de la 67e session de l'Assemblée générale des Nations Unies.

Ces différentes propositions sont toutefois rejetées par la plupart des pays occidentaux.

De manière schématique, on peut distinguer **trois conceptions** au niveau international :

- celle défendue par certains pays dits « libéraux », comme la Suède ou les Pays-Bas, qui sont très attachés à l'espace de liberté que représente l'Internet et hostiles à toute forme de réglementation du cyberespace ;

- la conception portée par la Chine et la Russie, qui faisant la promotion de règles contraignantes pour les Etats dans le cyberespace visent non seulement à renforcer les mesures relatives à la défense et à la sécurité des systèmes d'information, mais aussi à réglementer le contenu même des informations[2], ce qui est évidemment inacceptable pour la majorité des pays attachés aux principes de la liberté d'expression et de protection de la vie privée ;

- la France se situe dans une position médiane : elle est favorable à un renforcement de la gouvernance du cyberespace et à un minimum de régulation, par exemple pour protéger le droit d'auteur, mais dans le même temps elle s'oppose au concept de « sécurité de l'information ».

Par ailleurs, il ne faut pas sous-estimer les difficultés juridiques et pratiques soulevées par l'idée d'un traité international sur la cybersécurité, qui interdirait par exemple l'utilisation de capacités offensives ou la cyberguerre.

---

[1] *« China, Russia and Other countries submit the document of International Code of Conduct for Information Security to the United Nations »*, site du ministère des affaires étrangères de la République populaire de Chine, 13 septembre 2009

[2] *Une telle conception se retrouve par exemple dans la proposition russe intitulée « Convention on International Information Security (concept) », présentée lors du Sommet d'Ekaterinbourg, les 21 et 22 septembre 2011*

Comment définir une « arme informatique » ? Quels seraient les moyens de contrôle et les sanctions éventuelles d'une violation de cette interdiction ?

Les discussions se concentrent désormais sur l'idée de promouvoir au niveau international **des mesures de confiance** ou des ***« bonnes pratiques »***, par le biais de mesures non contraignantes, qui comprendraient deux volets :

- d'une part, une liste de mesures concrètes, comme l'identification des autorités compétentes pour traiter les attaques visant les systèmes d'information, la mise en place d'échanges d'informations ou des exercices réguliers, voire la constitution d'un réseau au niveau international ;

- d'autre part, un engagement des Etats à traiter les attaques informatiques transitant par leur territoire.

Une telle orientation s'est ainsi nettement dégagée lors de la conférence internationale sur le cyberespace, organisée à Londres, les 1 et 2 novembre 2011.

La question se pose aujourd'hui de savoir quelle serait l'enceinte la plus appropriée pour élaborer ces mesures de confiance.

L'**ONU** a adopté plusieurs documents concernant les technologies de l'information et de la communication et leurs aspects relatifs à la sécurité.

La première commission du désarmement et de la sécurité internationale de l'Assemblée générale des Nations Unies a adopté plusieurs résolutions et elle a constitué un groupe d'experts gouvernementaux. Ce groupe a présenté en 2010 un rapport appelant à poursuivre la concertation entre Etats sur des normes éventuelles relatives à l'utilisation des technologies de l'information et de la communication par les Etats, à adopter des mesures de confiance, de stabilité et de réduction des risques, à échanger des informations sur les législations nationales et les stratégies de sécurité nationales relatives aux technologies de l'information et de la communication et à définir des moyens d'aider les pays les moins développés à renforcer leurs capacités.

Dans sa résolution 65/41, adoptée en novembre 2011, l'assemblée générale des Nations Unies a décidé de la reprise des travaux du groupe d'experts gouvernementaux en 2012. Ces échanges devraient porter notamment sur la définition de mesures de confiance visant à renforcer la sécurité ou la recherche d'un consensus sur des normes de comportement dans le cyberespace.

La récente divulgation par la presse de l'utilisation par les Etats-Unis d'armes informatiques à des fins offensives à l'encontre de l'Iran, risque toutefois de remettre en cause cette démarche, puisqu'elle met en lumière l'utilisation par la première puissance mondiale de cyber-armes à l'encontre d'installations nucléaires étrangères en-dehors de tout cadre légitimant cette action vis-à-vis de la communauté internationale.

L'Union internationale des télécommunications (UIT), organisation spécialisée de l'ONU dont la vocation première est la normalisation en matière de télécommunications, a organisé, en liaison avec l'Assemblée générale des Nations unies et sur deux sessions qui se sont déroulées en 2003 et 2005, le sommet mondial sur la société de l'information, au cours duquel a été abordée la question de la gouvernance de l'internet.

L'UIT travaille à l'établissement d'un cadre international pour la promotion de la cybersécurité (Programme mondial cybersécurité*)* et a créé en 2008 un groupe d'experts de haut niveau chargé de proposer une stratégie à long terme englobant les mesures légales, les mesures techniques visant à remédier aux failles des produits logiciels, ainsi que la prévention et la détection des attaques informatiques et la gestion de crise.

Sous l'impulsion de son Secrétaire général, l'UIT souhaite renforcer son rôle en matière de cybersécurité, notamment dans la perspective d'une révision du règlement des télécommunications internationales, en novembre 2012. Le Secrétaire général de l'UIT a même évoqué en 2010 l'idée d'un traité international interdisant la cyberguerre.

Cette volonté de l'UIT est soutenue par la Chine et la Russie, qui souhaitent utiliser cette enceinte comme un des vecteurs de leur approche de la cybersécurité, ainsi que par la majorité des pays en voie de développement.

A l'inverse, les pays occidentaux, dont la France, s'opposent à l'idée de reconnaître un fondement juridiquement contraignant à l'action de l'UIT sur la cybersécurité. En revanche, l'UIT pourrait d'après eux jouer un rôle utile d'aide au développement de capacités nationales (création de CERT, établissement de stratégies, etc.), notamment en direction des pays en voie de développement.

Dans le cadre de sa présidence du **G8** en 2011, la France a inscrit pour la première fois la question d'Internet à l'ordre du jour d'un Sommet du G8. L'objectif était que les chefs d'État et de gouvernement puissent discuter du développement d'Internet, de son impact sur la croissance économique ou sur la promotion des droits de l'homme et des libertés démocratiques à la lumière notamment des « printemps arabes ».

Un Forum e-G8 a été organisé à Paris, les 24 et 25 mai, afin de réunir les grands acteurs des technologies de l'information et d'Internet issus du secteur privé et de la société civile. Ce forum a offert aux participants l'occasion de s'exprimer sur les défis et les opportunités qu'ils estiment pertinents pour l'avenir d'Internet.

La déclaration adoptée par les chefs d'Etat ou de gouvernement du G8, lors du Sommet de Deauville, les 26-27 mai 2011, contient un chapitre consacré à l'Internet. Cette déclaration rappelle les principes d'ouverture, de transparence et de liberté sur lesquels repose l'Internet, mais aussi la nécessité de prévoir des règles afin d'assurer notamment la protection de la propriété

intellectuelle, la protection des données à caractère personnel et de la vie privée ou encore la lutte contre la pédopornographie.

Dans le paragraphe consacré à la sécurité des réseaux et des services (paragraphe n°17), il est indiqué qu'*« une attention particulière doit être accordée à toutes les formes d'attaque contre l'intégrité des infrastructures, des réseaux et des services, y compris les attaques liées à la prolifération de logiciels malveillants et aux activités impliquant des réseaux d'ordinateurs contrôlés par un tiers sur l'Internet »* et qu'*« il est d'une importance cruciale de promouvoir la sensibilisation des utilisateurs et (…) de renforcer la coopération internationale afin de protéger les ressources vitales, les technologies de l'information et de la communication et d'autres infrastructures connexes »*.

Cette déclaration n'a toutefois pas débouché sur des actions concrètes.

L'**OCDE** s'est également préoccupée sous l'angle économique des attaques informatiques visant les entreprises et de leur impact sur l'économie. Dès 1992, l'OCDE a publié des lignes directrices relatives à la sécurité des systèmes d'information, qui ont été mises à jour en 2001, et plusieurs documents ont été publiés, portant notamment sur la protection des infrastructures d'information critiques[1].

L'action de l'**OSCE** en matière de cybersécurité est plus récente. Elle tient principalement à la volonté des Etats-Unis de promouvoir cette enceinte, véritable « machine à fabriquer de la confiance » et qui a joué un rôle important durant la « guerre froide », afin d'établir des mesures de confiance dans le cyberespace, en particulier avec la Russie.

Un comité cybersécurité et un groupe de travail dédié à la cybersécurité ont été constitués au sein de l'OSCE et ce groupe a notamment pour fonction de préparer l'établissement d'une liste de mesures de confiance et de sécurité pour le cyberespace.

Faute de véritable expertise sur la cybersécurité, cette organisation ne devrait toutefois rester qu'un simple forum d'échange entre les Etats.

Dans le cadre du **Conseil de l'Europe**, une convention dite de « Budapest » a été adoptée le 23 novembre 2001 en matière de lutte contre la cybercriminalité. Cette convention constitue le premier traité international qui définit les infractions pénales commises par l'intermédiaire d'Internet et d'autres réseaux informatiques. Elle porte en particulier sur les infractions portant atteinte aux droits d'auteurs, la fraude liée à l'informatique, la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Elle contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception.

---

[1] *Voir par exemple les recommandations sur la protection des infrastructures d'information critiques du 30 juin 2008*

A ce jour, cette convention a été ratifiée par trente cinq pays, dont la France et la plupart des pays de l'Union européenne, ainsi que par plusieurs pays non membres du Conseil de l'Europe, à l'image des Etats-Unis. En revanche, ni la Russie, ni la Chine, n'ont signé ce traité, ce qui en limite beaucoup la portée.

Enfin, un très grand nombre de **CERT** (*Computer emergency response team*) ont été mis en place dans le monde entier. Ces structures permanentes d'alerte et d'assistance sont chargées d'assurer, pour le compte des organismes qui s'y sont rattachés (administrations, centres de recherche, entreprises), une double mission d'information sur les vulnérabilités, les menaces en cours et les moyens d'y parer, et d'assistance en vue de résoudre les incidents. La France est dotée, comme de nombreux autres pays, d'un CERT gouvernemental, dénommé CERTA, dont la vocation est l'assistance aux administrations et aux opérateurs d'infrastructures vitales. Les CERT gouvernementaux, ainsi que les CERT dédiés au domaine militaire, constituent des capacités essentielles en matière de cyberdéfense.

Dès 1990, l'utilité de procéder à des **échanges entre les différents CERT** a été reconnue, avec la création d'une **enceinte internationale**, le *Forum of incident response and security teams* (**FIRST**).

Le FIRST a pour buts de favoriser la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d'incident de sécurité informatique, de fournir un moyen de communication commun pour la diffusion de bulletins et d'alertes sur des failles potentielles et les incidents en cours, d'aider au développement des activités de ses membres en matière de recherche et d'activités opérationnelles, et de faciliter le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques. Il organise une conférence annuelle internationale consacrée au traitement des incidents de sécurité et aux échanges d'expérience et d'expertise dans ces domaines.

Aujourd'hui, **le FIRST fédère près de 250 CERT répartis de par le monde**.

Une **enceinte spécifique,** l'**EGC** (*European Government Computer Security Incident Response Team*), a été créée par **certains pays européens** pour regrouper de manière informelle leurs structures gouvernementales. Le CERTA, CERT gouvernemental français, y participe avec ses homologues allemand, britannique, néerlandais, suisse, suédois, finlandais et norvégien.

L'EGC a pour but d'encourager le développement conjoint des mesures pour résoudre des incidents de sécurité de grande ampleur et de faciliter le partage d'informations et les échanges technologiques concernant les incidents de sécurité informatique, les menaces liées à des codes malveillants ainsi que les vulnérabilités des systèmes d'informations. L'EGC s'efforce également d'identifier des domaines de compétences spécialisés et d'expertise qui peuvent être partagées au sein du groupe, ainsi que des projets de coopération en matière de recherche et développement.

2. Une priorité de l'OTAN qui tarde à se concrétiser

Le thème de la cyberdéfense a retenu l'attention de l'OTAN dès le Sommet de Prague, en 2002, dont la déclaration finale préconisait un renforcement des capacités de l'Alliance contre les attaques informatiques.

L'OTAN s'est préoccupée dans un premier temps de la protection de ses propres systèmes d'information et de communication, et elle a mis en place à cet effet une structure spécifique : le centre technique de la capacité OTAN de réaction aux incidents informatiques (*Nato computer incident response capability – NCIRC*).

Ce centre NCIRC est responsable de la fourniture des services techniques et opérationnels de cybersécurité pour l'ensemble des réseaux et systèmes d'information et de communication propres à l'Alliance atlantique. Il doit permettre de traiter et de signaler les incidents et d'apporter son appui aux responsables de la gestion des systèmes. Par ailleurs, il a pour tâche de centraliser et de coordonner le traitement des incidents en un point unique, afin d'éviter toute duplication.

Les évènements survenus en Estonie au printemps 2007 ont amené l'OTAN à s'interroger sur son rôle, en tant qu'alliance défensive, en cas d'attaque contre l'un de ses membres.

Lors du sommet de Bucarest, d'avril 2008, les chefs d'Etat et de gouvernement des pays de l'Alliance ont souligné « *la nécessité pour l'OTAN et pour les pays de protéger les systèmes d'information clés conformément à leurs responsabilités respectives, de mettre en commun les meilleures pratiques, et de mettre en place une capacité visant à aider, sur demande, les pays de l'Alliance à contrer les cyberattaques* ».

En 2008, une autorité de contrôle de la cyberdéfense a été créée (*Cyber Defense Management Authority – CDMA*).

Les cyberattaques sont désormais une menace prise en compte dans le nouveau **concept stratégique de l'Alliance atlantique**, adopté lors du Sommet de Lisbonne en novembre 2010.

L'OTAN s'est dotée en janvier 2011 d'un **concept en matière de cyberdéfense,** décliné en juin 2011 en **une politique.** En octobre 2011, les ministres de l'OTAN ont approuvé un plan d'action, qui prévoit des actions concrètes.

Ce nouveau concept de cyberdéfense vise tout d'abord à **renforcer la sécurité des systèmes d'information de l'Alliance**, afin de la mettre à niveau face à la menace, grâce à l'amélioration des normes et des procédures de sécurité, et à une gestion plus centralisée.

La politique cyber de l'OTAN se veut globale, conformément au concept de *« cyberdéfense en profondeur »* promu par la France, c'est-à-dire qu'elle vise à compléter la défense traditionnelle des réseaux informatiques

par différents mécanismes de détection précoce des menaces, de diversion des cyberattaques et de limitation des effets néfastes de ces attaques. Elle inclut notamment des exercices réguliers, des tests de vulnérabilité et la formation.

Elle a également pour objectif de **renforcer la capacité de l'OTAN à coordonner l'assistance aux alliés subissant une attaque informatique d'importance, le cas échéant à l'aide d'équipes projetables**.

Le partage des responsabilités entre l'OTAN et les nations, qui conservent la charge de la protection de leurs propres systèmes d'information, a été défini de manière à bien délimiter le périmètre des systèmes dont la protection incombe à l'OTAN.

Dans le cadre de la réforme actuelle des agences de l'OTAN, il est également prévu de créer une nouvelle agence, qui doit regrouper la gestion de l'ensemble des systèmes d'information et de communication dépendants notamment de l'Agence de communication et des systèmes d'information de l'OTAN (*Communication and Information Systems Services Agency* – NCSA).

L'OTAN mène aussi depuis quelques années des exercices cyber. Ainsi, le dernier exercice, dénommé « Cyber coalition 2011 », qui s'est déroulé du 13 au 15 décembre 2011, a consisté à tester les capacités techniques et opérationnelles de l'Alliance en matière de cyberdéfense. Cet exercice était basé sur une situation de crise fictive dans laquelle tous les pays participants étaient confrontés à des cyberattaques simulées. 23 pays de l'OTAN et six pays partenaires ont participé à cet exercice.

Enfin, cette politique définit également les principes de la coopération, dans le domaine de la cyberdéfense, entre l'OTAN, les pays partenaires, les organisations internationales, le secteur privé et le monde universitaire.

Pour autant, **l'OTAN n'est pas complètement armée face à cette menace.**

D'ailleurs, l'OTAN a été la cible de plusieurs attaques informatiques en avril 2010, attaques attribuées à la mouvance *Anonymous* et même l'ordinateur personnel du Secrétaire général de l'OTAN a été piraté.

Ainsi, la principale unité informatique de l'Alliance n'est toujours pas opérationnelle 24 heures sur 24, 7 jours sur 7 et elle n'assure pas encore la sécurité de l'ensemble des systèmes et des réseaux de l'OTAN.

Lors du dernier Sommet de Chicago, de mai 2012, les chefs d'Etat et de gouvernement des pays de l'Alliance ont rappelé l'objectif d'une pleine capacité opérationnelle du centre de l'OTAN de réaction aux incidents informatiques d'ici la fin de l'année 2012.

Le 8 mars 2012, un contrat de 58 millions d'euros a été attribué par l'OTAN à l'américain Northrop Grumman, associé aux entreprises Finmeccanica, SELEX Elsag et VEGA, pour la mise en place de la capacité opérationnelle de l'OTAN en matière de réponse aux cyberattaques.

Toutefois, **il est désormais clair que cet objectif ne pourra pas être atteint dans ce délai et nécessitera encore plusieurs années pour l'être pleinement.**

Plus généralement, **l'OTAN doit encore déterminer quelle attitude adopter pour répondre à des cyberattaques lancées contre l'un des Etats membres.**

Peut-on invoquer **l'article 5** du traité de Washington en cas de cyberattaque ? Une « attaque informatique » peut-elle être assimilée à un « acte de guerre » et comment identifier l'agresseur ? Les mesures de rétorsion doivent-elles se limiter à des moyens cybernétiques, ou bien peut-on également envisager des frappes militaires conventionnelles ?

Il n'y a pas encore de réponses claires à ces questions, comme votre rapporteur a pu le constater lors de ses entretiens au siège de l'OTAN à Bruxelles avec les principaux responsables chargés de ces questions.

Lors du dernier Sommet de l'OTAN, qui s'est tenu à Chicago, le 20 mai 2012, les chefs d'Etat et de gouvernement des pays membres de l'Alliance atlantique ont adopté une déclaration, dont le point 49 est consacré à **la cyberdéfense**.

Cette déclaration insiste d'abord sur **la montée en puissance de la menace** : *« Le nombre de cyberattaques continue de s'accroître de manière significative et leur niveau de sophistication et de complexité ne cesse d'évoluer ».*

Elle traduit également **l'engagement des pays membres de l'OTAN à renforcer les capacités de l'Alliance atlantique en matière de cyberdéfense, tout en rappelant que les Etats membres restent responsables de la protection de leurs propres systèmes d'information et de communication** :

« Sur la base des capacités existantes de l'OTAN, les éléments critiques de la capacité opérationnelle totale (FOC) de la capacité OTAN de réaction aux incidents informatiques (NCIRC), y compris la protection de la plupart des sites et des utilisateurs, seront en place d'ici la fin 2012. Nous nous sommes engagés à fournir les ressources et à mener à bien les réformes nécessaires pour mettre en place une capacité centralisée de cyberprotection pour tous les organismes de l'OTAN, de manière à garantir que les moyens que nous investissons collectivement dans l'OTAN sont protégés par des capacités de cyberdéfense renforcées. Nous allons continuer d'intégrer des mesures de cyberdéfense dans les structures et les procédures de l'Alliance et, à titre individuel, nous restons attachés à recenser et à mettre en place des capacités nationales de cyberdéfense qui renforcent la collaboration et l'interopérabilité au sein de l'Alliance, y compris dans le cadre des processus OTAN de planification de défense. Nous continuerons de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever ».

Enfin, la déclaration reconnaît **l'importance de la coopération avec d'autres partenaires ou organisations, et en premier lieu avec l'Union européenne** :

« Pour faire face aux menaces qui pèsent sur la cybersécurité et pour améliorer notre sécurité commune, nous sommes déterminés à travailler avec les pays partenaires concernés, au cas par cas, et avec des organisations internationales, entre autres l'UE, comme convenu, le Conseil de l'Europe, l'ONU et l'OSCE en vue d'accroître la coopération concrète. En outre, nous tirerons pleinement parti de l'expertise offerte par le Centre d'excellence pour la cyberdéfense en coopération en Estonie ».

Un **accord de coopération et de coordination technique** sur la cyberdéfense a ainsi été conclu entre la France (ANSSI et état-major des armées) et l'Alliance atlantique, le 30 septembre 2011, qui prévoit des échanges d'informations et de bonnes pratiques, l'assistance en situation de crise et la participation à des activités conjointes.

En revanche, on peut regretter l'insuffisante coopération entre l'OTAN et l'Union européenne dans ce domaine.

Même si l'établissement d'une coopération formelle se heurte à des difficultés politiques, en raison du différend chypriote, mais aussi de la difficulté pour l'OTAN de trouver un interlocuteur unique du côté de l'Union européenne en raison de la dispersion des responsabilités au niveau européen, **il semble souhaitable de renforcer la coopération entre l'OTAN et l'Union européenne dans ce domaine**, dans un souci de complémentarité et de mutualisation.

Cela pourrait passer par un renforcement des échanges entre l'état-major de l'OTAN et celui de l'Union européenne, entre le NCIRC et le CERT de l'Union européenne, entre le commandement allié chargé de la transformation (ACT) et l'agence européenne de défense (AED) ou encore entre le centre d'excellence pour la cyberdéfense en coopération de Tallinn et l'agence européenne chargée de la securité des réseaux et de l'information (ENISA).

Sept pays alliés[1] ont décidé en 2008 de contribuer à la création d'un **centre d'excellence sur la cyberdéfense**. Plusieurs pays, dont les Etats-Unis, ont décidé de les rejoindre portant à onze à ce jour les pays représentés[2] au sein du centre.

Ce centre n'est pas à proprement parler un organisme de l'OTAN mais il a reçu une homologation de l'Alliance atlantique en 2008. Constitué à partir d'une capacité estonienne déjà existante, ce centre, situé à Tallin, est constitué d'une trentaine d'experts provenant des pays impliqués. Comme votre rapporteur a pu le constater lors d'un déplacement à Tallin, en marge de

---

[1] *Allemagne, Espagne, Estonie, Italie, Lettonie, Lituanie et Slovaquie.*

[2] *Pologne, Hongrie, Pays-Bas et Etats-Unis. Des discussions sont également en cours avec la Turquie.*

l'assemblée parlementaire de l'OTAN, au cours de laquelle il a eu l'occasion de visiter le centre d'excellence et de s'entretenir avec son commandant, le colonel Ilmar Tamm, ce centre n'a pas de vocation opérationnelle mais s'apparente plutôt à un centre de recherche. Son objectif est de réunir au profit de l'Alliance l'expertise en matière de risques cybernétique, d'élaboration d'une doctrine, de retour d'expérience et de formation d'experts. Ses travaux portent principalement sur le cadre juridique national et international, la doctrine et les concepts, ainsi que sur la protection des infrastructures critiques.

Alors que onze pays membres de l'OTAN sont aujourd'hui représentés au sein du centre d'excellence sur la cyberdéfense, dont les Etats-Unis, on peut regretter l'absence de toute présence française, comme d'ailleurs de l'Union européenne en tant qu'organisation.

Alors que la France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN, il semblerait souhaitable pour votre rapporteur que la France soit représentée au sein du centre d'excellence sur la cyberdéfense.

Une telle présence serait cohérente avec le renforcement de notre participation et de notre influence au sein de l'Alliance atlantique, conséquence de la réintégration pleine et entière de la France au sein des structures de commandements et organes de l'OTAN décidée en 2009, mais aussi de la volonté de notre pays de s'affirmer sur le plan international comme un acteur important sur ce dossier.

Pourquoi ne pas envisager également une présence de l'Union européenne au sein du centre d'excellence sur la cyberdéfense ?

3. Une implication encore insuffisante de l'Union européenne

L'Union européenne a un rôle important à jouer en matière de protection des systèmes d'information car une grande partie des normes relatives à ce domaine relèvent de ses compétences.

Par ailleurs, l'Union européenne a elle-même été la cible de plusieurs attaques informatiques ces dernières années, à l'image de l'attaque informatique de janvier 2011 visant le marché européen du carbone, où les entreprises peuvent échanger leurs certificats de quotas d'émission de CO2, qui n'est redevenu complètement opérationnel que trois mois plus tard.

Toutefois, malgré l'adoption d'un grand nombre de textes, l'action concrète de l'Union européenne dans ce domaine est restée jusqu'à présent relativement limitée.

Ces dernières années, les instances européennes ont adopté de **nombreux documents d'orientations ou de programmes** intéressant directement ou indirectement la sécurité des systèmes d'information.

Pour la période récente, on peut notamment mentionner :

- la stratégie dite « i2010 » (« Une société de l'information pour la croissance et l'emploi ») exposée dans une communication de la Commission européenne du 1er juin 2005, et qui confirme l'importance de la sécurité des réseaux ;

- la communication de la Commission du 31 mai 2006, intitulée « Une stratégie pour une société de l'information sûre – dialogue, partenariat et responsabilisation », qui contient notamment une évaluation comparative des politiques nationales relatives à la sécurité des réseaux et de l'information mais qui ne propose aucune action concrète ;

- la communication de la Commission de mars 2009 relative à la « protection des infrastructures d'information critiques » qui fixe des objectifs prioritaires dans le domaine de la sécurité des systèmes d'information et qui a débouché sur un plan d'action, adopté en avril 2009, comprenant cinq axes. Parmi les différentes mesures envisagées, la Commission européenne se donne notamment pour objectif le développement par chaque Etat membre d'un CERT opérationnel, l'organisation d'exercices de gestion de crise cyber aux niveaux national et européen ou encore la création d'un forum d'échange public-privé européen, etc. Ce plan d'action a été approuvé par le Conseil en décembre 2009 ;

- la communication de la Commission de mai 2010 intitulée « Une stratégie numérique pour l'Europe », qui aborde l'ensemble des enjeux liés au développement de la société de l'information en Europe. Cette communication souligne à nouveau la nécessité d'une mise en œuvre rapide et efficace du plan d'action de l'Union européenne pour la protection des infrastructures d'information critiques ;

- une nouvelle communication de la Commission européenne relative à « la protection des infrastructures d'information critiques » de mars 2011, qui reprend et développe les cinq axes de la communication de mars 2009 et introduit de nouvelles propositions, telles que le développement d'un plan européen de continuité en cas de crise cyber et la création d'un groupe de travail commun Union européenne-Etats-Unis sur la cybersécurité et la cybercriminalité. Cette communication a fait l'objet de conclusions du Conseil en mai 2011, qui soulignent notamment l'importance stratégique de l'industrie européenne des télécommunications et de l'industrie de la sécurité des réseaux et de l'information en vue de la protection durable des infrastructures d'information critiques européennes.

On peut toutefois observer que **ces documents fixent des objectifs très généraux, mais ne paraissent pas encore en mesure de se traduire rapidement par des initiatives concrètes.**

Il faut également souligner que des initiatives ont été prises au niveau européen en matière de lutte contre la cybercriminalité, avec par exemple

l'adoption, le 24 février 2005, d'une décision-cadre relative aux attaques visant les systèmes d'information.

De même, une directive a été adoptée le 8 décembre 2008 relative à la protection des infrastructures critiques européennes, mais ce texte, qui se limite aux secteurs de l'énergie et des transports, se contente d'appeler les Etats-membres à identifier les infrastructures critiques concernées et à prévoir des mesures en matière de sécurité, sans entrer véritablement dans le détail des mesures nécessaires.

Par ailleurs, la cyberdéfense est également un thème de travail récent de la politique de sécurité et de défense commune, notamment au sein de l'Agence européenne de défense, qui a constitué une *« Project Team »* sur ce sujet. Toutefois, les travaux de l'Union européenne dans ce domaine sont encore très embryonnaires et n'ont pas encore débouché sur des réalisations concrètes.

Ainsi, à l'image de l'OTAN, il n'existe aucun consensus entre les vingt-sept Etats membres de l'Union européenne sur la mise en œuvre de la « clause de défense mutuelle » contenue dans le traité de Lisbonne, en cas d'attaque informatique majeure contre un Etat membre.

De manière générale, malgré l'adoption de nombreux documents ou plans d'action, **l'Union européenne, et la Commission européenne en particulier, ne semblent pas encore avoir pris la mesure de l'importance des enjeux liés à la sécurité des systèmes d'information, comme d'ailleurs de nombreux pays européens.**

On peut mentionner **trois principales lacunes.**

Tout d'abord, **l'absence de véritable stratégie globale du cyberespace à l'échelle européenne**.

Actuellement, les discussions au niveau européen se concentrent sur l'élaboration d'une nouvelle « stratégie européenne de sécurité de l'Internet », et plus récemment d'une « stratégie européenne de cybersécurité », qui devrait prendre la forme d'une communication de la Commission européenne dont la publication devrait intervenir en septembre 2012.

Centrée sur l'enjeu de la sécurité de l'Internet, considéré comme la première des infrastructures critiques civiles en Europe, mais également sur la lutte contre la cybercriminalité et la coopération internationale, cette stratégie s'inscrit dans la continuité des travaux menés ces dernières années au sein de l'Union européenne en matière de sécurité des réseaux et de l'information. Cependant, la sécurité de l'Internet ne constitue qu'un des éléments de la réponse européenne aux défis et enjeux du cyberespace.

Ensuite, **une dispersion des acteurs**.

Ainsi, au sein de la Commission européenne, on assiste à une concurrence entre les différentes directions générales pour le pilotage des enjeux autour de la cybersécurité au niveau de l'Union européenne. Si la

direction générale de la Société de l'information et des médias est principalement chargée de la mise en œuvre de la stratégie numérique pour l'Europe, d'autres directions générales, à l'image de la direction générale « Affaires intérieures » pour le volet relatif à la lutte contre la cybercriminalité ou encore la direction générale « marché intérieur » pour les aspects relatifs aux règles du marché intérieur, interviennent également dans ce domaine.

Par ailleurs, on peut déplorer une insuffisante coordination entre les aspects qui concernent des matières communautaires et qui relèvent de la Commission européenne et ceux qui touchent à des matières intergouvernementales, à l'image de la politique étrangère ou de la politique de sécurité et de défense commune, qui relèvent du Haut représentant pour l'action extérieure et du service européen pour l'action extérieure.

Enfin, on constate **un manque d'efficacité**.

Ainsi, à l'image de l'OTAN, **l'Union européenne ne paraît pas encore en mesure d'assurer la protection de l'ensemble de ses propres réseaux et systèmes d'information.**

L'Union européenne s'est certes dotée, le 10 juin 2011, d'un CERT (« Computer Emergency Response Team ») européen, chargé de prévenir et de répondre aux attaques informatiques visant les réseaux ou systèmes des institutions européennes, des agences ou des autres organes qui lui sont rattachés.

Mais cette structure, qui ne compte que dix agents, n'en est encore qu'au stade de la préfiguration et est encore très loin d'assurer une protection de l'ensemble des réseaux et systèmes de l'Union européenne.

Par ailleurs, la coordination et l'efficacité des différents outils, mécanismes et politiques, à la fois réglementaires et incitatifs, mis en place à l'échelle européenne pour encourager la prise en compte par les Etats membres des enjeux liés à la protection des systèmes d'information mériteraient d'être notablement renforcés.

Ainsi, l'Union européenne dispose d'un instrument spécialisé à travers l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'**ENISA** (*European Network and Information Security Agency*), qui a été créée en 2004 avec un mandat initial d'une durée de cinq ans.

Installée à Heraklion, en Crète, **l'ENISA s'est vue assigner des missions très vastes,** que l'on peut regrouper en trois catégories :

- conseiller et assister, en tant qu'agence d'expertise technique, la Commission européenne et les États membres en matière de sécurité des systèmes d'information, notamment au travers de « guides de bonnes pratiques » ;

- soutenir les Etats membres et les institutions européennes dans le développement de capacités pour répondre aux menaces pesant sur la sécurité des systèmes d'information ;

- encourager la coopération entre les Etats membres, notamment par des exercices communs.

Cette agence européenne n'a donc pas de compétences opérationnelles mais plutôt une mission de conseil et de recommandation. Elle dispose d'environ 60 agents et d'un budget de 8,5 millions d'euros en 2012.

L'ENISA a fait l'objet d'une **évaluation externe** demandée par la Commission qui en a publié le résultat en juin 2007. Le groupe d'experts externe a conclu que **les activités de l'ENISA paraissaient « *insuffisantes pour atteindre le niveau élevé d'impact et de valeur ajouté espéré* »** et que sa visibilité était en dessous des attentes. L'évaluation recense divers handicaps liés à son organisation, aux ambiguïtés du mandat originel, à sa localisation éloignée, à l'effectif et à la rotation importante du personnel, aux relations difficiles entre le conseil d'administration et la direction de l'agence. Elle souligne un risque d'affaiblissement rapide et de perte de réputation si l'efficacité n'était pas améliorée.

Le Livre blanc sur la défense et la sécurité nationale de 2008 a souligné également que « *l'efficacité de l'agence européenne ENISA devra être très notablement accrue* », notamment pour permettre à la Commission européenne de mettre en place un volet « sécurité des systèmes d'information » dans toutes les réalisations des institutions européennes.

On peut toutefois souligner que, ces derniers mois, l'agence a publié des rapports intéressants avec des recommandations concrètes, par exemple sur les systèmes de contrôle industriels et les SCADA ou encore la cybersécurité maritime. En outre, dans le cadre du groupe de travail sur les exercices piloté par l'ENISA, un premier exercice européen de crise cyber, intitulé « Cyber Europe 2010 », a été organisé en 2010.

Le mandat de l'ENISA a été prolongé jusqu'en septembre 2013 et une proposition de règlement visant à modifier et à étendre le mandat de cette agence est actuellement en discussion au niveau européen.

On peut également relever l'adoption, **en novembre 2009**, de **la directive cadre du « Paquet Télécom »** modifiant la régulation des communications électroniques en Europe[1].

Cette directive contient une disposition (article 13 bis) contraignant les opérateurs de télécommunications à notifier aux autorités nationales compétentes toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services. Elle introduit également l'obligation de mise en œuvre de mesures de sécurité minimales par

---

1 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009

les opérateurs, les autorités nationales étant chargées de s'assurer que les opérateurs respectent ces obligations.

Cette directive cadre a été transposée en France par le biais de l'ordonnance du 24 août 2011, qui a modifié la loi du 6 janvier 1978 dite « informatique et libertés », en prévoyant notamment l'obligation pour les opérateurs de télécommunications de notifier à la CNIL toute faille de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

En définitive, il semble indispensable que l'Union européenne s'implique plus activement sur les questions liés à la protection des systèmes d'information.

C. LES FREINS À LA COOPÉRATION INTERNATIONALE

Si, face à une menace qui s'affranchit des frontières, la coopération internationale est une nécessité, cette coopération se heurte toutefois en pratique à de nombreux obstacles.

On peut à cet égard mentionner trois principales limites.

La première limite résulte du **manque de confiance** qui existe au niveau international. Etant donné la difficulté d'identifier précisément l'origine des attaques informatiques et les soupçons qui pèsent sur l'implication de certains Etats, la plupart des pays sont réticents à partager des informations ou des connaissances, par crainte d'affaiblir leurs propres moyens de protection face à ces attaques.

Selon certains, *« il n'existe pas de véritables alliés dans le cyberespace »*.

Un deuxième frein tient aux **différentes conceptions** qui existent entre les Etats, en particulier entre ceux, comme les pays occidentaux, qui sont attachés à l'espace de liberté que représente Internet, et d'autres, comme la Russie ou la Chine, qui, inquiets du rôle joué par l'Internet et les réseaux sociaux notamment à la lumière des révolutions du « printemps arabe », cherchent à restreindre les droits et libertés sur ces nouveaux médias et à contrôler le contenu même des informations.

Enfin, la dernière limite s'explique par les préoccupations partagées par la plupart des Etats de **préserver leur souveraineté nationale.** Cela est particulièrement vrai concernant la conception des produits de sécurité informatique, notamment ceux destinés à protéger l'information de souveraineté.

Ainsi, on constate que de nombreux Etats privilégient les coopérations bilatérales avec leurs proches alliés et hésitent à évoquer ces sujets dans un cadre multilatéral.

III. LA FRANCE A COMMENCÉ À COMBLER SON RETARD MAIS NOTRE DISPOSITIF CONNAÎT ENCORE D'IMPORTANTES LACUNES

S'il y a encore quelques années, la France enregistrait un important retard, le Livre blanc de 2008 a donné une réelle impulsion à la politique française en matière de protection des systèmes d'informations. Malgré plusieurs avancées significatives, comme la création d'une agence nationale de sécurité des systèmes d'information ou l'élaboration d'une stratégie, notre dispositif connaît encore d'importantes lacunes.

A. UNE PRISE DE CONSCIENCE TARDIVE

1. Le constat sévère du rapport Lasbordes de 2006

Dans un rapport remis au Premier ministre, le 13 janvier 2006, intitulé : « *La sécurité des systèmes d'information – Un enjeu majeur pour la France* », notre ancien collègue député **Pierre Lasbordes** dressait un **constat sans complaisance des faiblesses de notre organisation et de nos moyens**, notamment au regard de nos partenaires européens les plus proches.

Il estimait ainsi que « ***la France accuse un retard préoccupant face aux impératifs de sécurité des systèmes d'information, tant au niveau de l'Etat qu'au niveau des entreprises, quelques grands groupes mis à part***».

● ***Une organisation marquée par la dispersion et l'autonomie des différents acteurs au sein des services de l'Etat***

L'une des principales faiblesses mise à jour par le rapport Lasbordes tenait à la conduite de la politique de sécurité des systèmes d'information, qui souffrait d'une grande dispersion des acteurs et à l'autorité insuffisante des structures chargées de la mettre en œuvre.

La France a défini en 1986 une politique d'ensemble de la sécurité des systèmes d'information, avec l'adoption d'une série de textes réglementaires instituant une commission et une délégation interministérielles, ainsi qu'un service central de la sécurité des services d'information.

Cette organisation a été revue avec l'attribution en 1996 au Secrétariat général de la défense nationale (SGDN) d'une responsabilité particulière dans le domaine de l'identification et de la surveillance des risques affectant la sécurité des systèmes d'information. Une direction centrale de la sécurité des services d'information (DCSSI), partie intégrante du SGDN, avait été créée par un décret du 31 juillet 2001.

Le rapport Lasbordes estimait cependant que *« la multiplication des acteurs publics, dont les missions se chevauchent et dont les textes fondateurs sont peu précis, donne une impression générale de confusion et d'éparpillement des moyens et des hommes. Dans cette nébuleuse, l'acteur*

public dédié, le SGDN et plus précisément la DCSSI, souffre d'un manque d'autorité et parfois de crédibilité auprès des publics concernés. Ces deux facteurs, l'éparpillement des moyens et le manque d'autorité du SGDN, nuisent à l'efficacité de l'Etat dans la définition et la mise en œuvre de la politique globale de sécurité des systèmes d'information ».

● ***Des moyens insuffisants***

Le deuxième constat principal du rapport Lasbordes tenait à l'insuffisance des moyens consacrés à la sécurité des systèmes d'information.

Il soulignait l'**effectif très restreint de la DCSSI**, limité à 100 personnes, qui ne lui permettait pas de répondre aux besoins identifiés dans le cadre de ses missions, que ce soit en matière de réalisation d'inspections au sein des ministères, de formation, de conseil aux administrations et aux entreprises.

● ***Des entreprises vulnérables***

Une large partie du rapport Lasbordes est consacrée au **monde de l'entreprise**, qu'il considère comme étant au cœur de la menace et de la problématique de la sécurité des systèmes d'information.

Il estime que d'une manière générale, **les entreprises françaises ont insuffisamment pris en compte la réalité de la menace** et ne se sont pas mises en situation de s'en protéger, quelques grands groupes mis à part. Les raisons évoquées tiennent au manque d'implication des directions générales, à la formation insuffisante des personnels en matière de risques informatiques, à l'absence d'identification pertinente des données sensibles ou à l'insuffisance des budgets dédiés à la sécurité des systèmes d'information.

● Le rapport Lasbordes concluait sur **six recommandations** :

- sensibiliser et former à la sécurité des systèmes d'information ;

- responsabiliser les acteurs, par la généralisation des chartes d'utilisateurs et la labellisation des fournisseurs de produits sécurisés ;

- renforcer la politique de développement de technologies et de produits de sécurité et définir une politique d'achat public en cohérence ;

- rendre accessible la sécurité des systèmes d'information à toutes les entreprises ;

- accroître la mobilisation des moyens judiciaires ;

- assurer la sécurité de l'Etat et des infrastructures vitales.

Il préconisait également une **réorganisation de la politique interministérielle de la sécurité des systèmes d'information** en séparant les fonctions d'autorité, confiées au SGDN, et les fonctions opérationnelles qui s'appuieraient sur les moyens de l'ancienne DCSSI renforcés et regroupés dans une structure nouvelle à statut d'établissement public industriel et commercial.

2. Le rapport Romani de 2008

En février 2008, la commission des affaires étrangères, de la défense et des forces armées du Sénat, présidée à l'époque par M. Josselin de Rohan, a souhaité s'intéresser à ce sujet et a confié à l'un de ses membres, M. Roger Romani, la mission de préparer un rapport sur la cyberdéfense.

Publié le 8 juillet 2008, le rapport d'information, intitulé « *Cyberdéfense : un nouvel enjeu de sécurité nationale* » présenté par notre ancien collègue estimait que ***« la France n'est ni bien préparée, ni bien organisée »*** face à la menace d'attaques informatiques.

D'après ce rapport**,** le manque de moyens, notamment en comparaison avec nos voisins britanniques ou allemands, se conjugue à l'absence d'une autorité centrale véritablement susceptible d'impulser et de coordonner une politique d'ensemble de la sécurité des systèmes d'information**.**

Enfin, si le rapport approuve les orientations très positives retenues par le Livre blanc, notamment la création de l'Agence de la sécurité des systèmes d'information, il estime que cette agence devra être impérativement dotée des moyens et de l'autorité permettant de mener une action plus résolue dans le domaine de la sécurité des systèmes d'information, et il formule plusieurs propositions en ce sens.

3. Le Livre blanc sur la défense et la sécurité nationale de 2008

Le Livre blanc sur la défense et la sécurité nationale de 2008 a marqué un véritable « tournant ». En effet, avec le Livre blanc, la **protection des systèmes d'information** est clairement définie comme une **composante à part entière de notre politique de défense et de sécurité**.

Le Livre blanc accorde, pour la première fois, une place importante à la menace représentée par les attaques informatiques.

Il estime en effet que *« le niveau quotidien actuel des agressions contre les systèmes d'information, qu'elles soient d'origine étatique ou non, laisse présager un potentiel très élevé de déstabilisation de la vie courante, de paralysie de réseaux critiques pour la vie de la nation, ou de déni de fonctionnement de certaines capacités militaires ».*

Aux yeux des rédacteurs du Livre blanc, la multiplication des tentatives d'attaques menées par des acteurs non étatiques dans les quinze ans à venir constitue une certitude, alors que « *plusieurs pays ont déjà défini des stratégies de lutte informatique offensive et se dotent effectivement de capacités techniques relayées par des pirates informatiques* ».

Le Livre blanc juge que des tentatives d'attaques étatiques dissimulées sont hautement probables et que des actions massives menées ouvertement sont également plausibles.

Le Livre blanc de 2008 définit aussi une nouvelle approche en matière de sécurité des systèmes d'information.

Il préconise ainsi « *le passage d'une stratégie de défense passive à une* ***stratégie de défense active en profondeur****, combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive* », une telle évolution supposant « *une forte impulsion gouvernementale et un changement des mentalités* ».

La **défense passive** peut être définie comme un simple recours aux systèmes automatiques de protection des réseaux (pare-feux, antivirus), placés à la frontière entre ceux-ci et l'extérieur. Ces outils sont indispensables, mais insuffisants, car ils ne sont pas infaillibles et peuvent être contournés puisqu'ils ne protègent que des menaces déjà identifiées contre lesquelles ils ont été conçus.

La **défense active** implique une **véritable capacité de surveillance des « frontières »** et l'**aptitude à s'adapter en permanence à une menace qui évolue de manière quotidienne,** de nouvelles vulnérabilités apparaissant en permanence.

Afin de renforcer la cohérence et la capacité propre des moyens de l'Etat, le Livre blanc prévoit la création d'**une agence chargée de la sécurité des systèmes d'information**. Relevant du Premier ministre et de la tutelle du SGDSN, cette agence *« mettra en œuvre une capacité centralisée de détection et de défense face aux attaques informatiques. Elle sera dotée des moyens de faire développer et d'acquérir les produits de sécurité essentiels à la protection des réseaux les plus sensibles de l'Etat. Elle sera également chargée d'assurer une mission de conseil du secteur privé, notamment dans les secteurs d'activité d'importance vitale »*.

Enfin, le Livre blanc évoque pour la première fois les **« capacités offensives »** : *« Dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace. Des règles d'engagement appropriées, tenant compte des considérations juridiques à ce nouveau milieu, devront être élaborées »*.

B. DE RÉELLES AVANCÉES DEPUIS 2008

Le Livre blanc sur la défense et la sécurité nationale de 2008 a permis de donner une réelle impulsion à la politique française en matière de défense et de protection des systèmes d'information.

En termes d'organisation, le Livre blanc a permis à cette politique d'être clairement identifiée, avec la création, en juillet 2009, de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information. Celle-ci a rendu publique, en février 2011, la stratégie de la France dans ce domaine.

Plusieurs ministères, et en particulier le ministère de la défense et les armées, ont mis en place une nouvelle organisation. Enfin, dans le droit fil des recommandations du Livre blanc, des capacités de détection et de protection ont commencé à être déployées dans les administrations.

1. La création de l'Agence nationale de la sécurité des systèmes d'information

Les rapports Lasbordes, Romani, ainsi que le Livre blanc de 2008 avaient préconisé la création d'une agence interministérielle chargée de la sécurité des systèmes d'information, en vue de renforcer la cohérence et la capacité propre des moyens de l'Etat.

Cette agence, dénommée « Agence nationale de la sécurité des systèmes d'information » (ANSSI), a été créée le 7 juillet 2009, par un décret du Premier ministre[1], sous la forme d'un service à compétence nationale.

Elle a remplacé la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense et nationale, tout en renforçant ses attributions, ses effectifs et ses moyens.

Cette agence relève du Premier ministre et elle est distincte des services du **SGDSN** tout en étant placée sous la **tutelle** directe du Secrétaire général de la défense et de la sécurité nationale, M. Francis Delon. Elle est dirigée par M. Patrick Pailloux.

Les prérogatives de l'ANSSI recouvrent les capacités en matière de prévention, de détection et de réaction aux attaques informatiques. L'agence n'a aucune compétence concernant les « aspects offensifs ». Par ailleurs, le ministère de la défense et les services spécialisés conservent des attributions particulières.

Les attributions de l'ANSSI recouvrent **six principales missions**.

En tant qu'autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI est chargée de **proposer les règles à appliquer pour la protection des systèmes d'information de l'Etat et de vérifier l'application des mesures adoptées.**

Ainsi, l'ANSSI est chargée de préparer la stratégie nationale en matière de sécurité des systèmes d'information, d'animer et de coordonner les relations avec les différents ministères, de préparer les textes législatifs et réglementaires intéressant la sécurité des systèmes d'information et la rédaction de référentiels, la labellisation de sécurité des produits et des prestations de service, l'organisation et le suivi de relations internationales et de relations industrielles, ainsi que l'instruction des dossiers de déclaration et d'autorisation relatifs aux produits réglementés.

---

[1] *Décret n°2009-834 du Premier ministre en date du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »*

L'ANSSI est ainsi chargée d'élaborer le **référentiel général de sécurité** (RGS), qui désigne l'ensemble des règles relatives aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui participent à la sécurité des informations et qui doivent respecter certaines fonctions, comme la signature électronique, l'authentification ou la confidentialité.

En matière de **cyberdéfense**, l'ANSSI est chargée de détecter et de réagir au plus tôt en cas d'attaque informatique.

Le **centre opérationnel de la sécurité des systèmes d'information** (COSSI), qui a été créé en 2003 et qui est opérationnel 7 jours sur 7, 24 heures sur 24 depuis 2005, assure la mise en œuvre de la fonction d'autorité de défense des systèmes d'information dévolue à l'ANSSI. Son action s'exerce en priorité au profit des administrations de l'Etat, ainsi que des opérateurs d'importance vitale. Le COSSI apporte son soutien et son expertise à la résolution des nombreux incidents de sécurité majeurs rencontrés par des ministères et les grandes entreprises. Il émet aussi des avis de sécurité, des alertes et des bulletins d'actualité sur les attaques en cours, qu'il met en ligne sur le site Internet de son centre d'expertise, le CERT gouvernemental français.

Le COSSI assure un service permanent de veille, de détection et d'alerte destiné à déceler les vulnérabilités susceptibles d'affecter la sécurité des systèmes d'information, à proposer des mesures de contournement nécessaires et à détecter les attaques visant les systèmes d'information de l'Etat. En cas d'incident, il assiste les services concernés en matière de prévention, de détection, de protection et de réaction. En cas d'attaque informatique majeure, il décide des mesures urgentes à faire appliquer par l'Etat et les opérateurs d'importance vitale.

Le COSSI assure, au niveau central, la planification des mesures de réponse aux attaques informatiques, notamment dans le cadre des plans VIGIPIRATE et PIRANET. Il organise des exercices afin d'évaluer les dispositifs techniques et organisationnels de prévention, de détection, de protection et de réaction mis en place, d'entraîner les personnels concernés et de mesurer le degré de préparation de la Nation.

LE PLAN PIRANET

Complémentaire au plan Vigipirate, le **plan Piranet** est **destiné à faire face à des attaques informatiques majeures, pouvant être d'origine terroriste, ayant touché les systèmes d'information de l'État ou d'opérateurs d'infrastructures d'importance vitale**, et à organiser la **réponse à ces attaques** :

- en mettant en œuvre un **dispositif d'alerte et d'intervention** ;

- en procédant au **confinement des attaques** ainsi qu'à la **remise en état des systèmes touchés** ;

- en transmettant également l'**alerte vers les services non affectés**, en leur indiquant les postures à prendre et les parades à mettre en place.

Le plan Piranet est l'un des piliers de la stratégie de défense informatique française. Il définit l'organisation et les processus de gestion de crise permettant à l'État de prendre les dispositions nécessaires. Il prévoit également l'application de mesures adaptées à une menace ou une attaque informatique d'ampleur. Ce plan est préparé et maintenu par l'ANSSI et le SGDSN et déclenché par le Premier ministre.

Le premier plan Piranet a été créé en 2002, peu après les attentats du 11 septembre 2001. Le dernier exercice « Piranet 2012 », qui s'est déroulé les 7, 8 et 9 février 2012, reposait sur le scénario d'une « crise informatique majeure », telle qu'une interruption totale de la connexion à l'Internet, et visait à tester la capacité de l'Etat à réagir et à se coordonner en cas d'attaques causant de graves dysfonctionnements des systèmes d'information de la Nation. Outre les services de l'Etat, des opérateurs d'importance vitale des secteurs de la santé, des transports et des communications électroniques ont été associés à cet exercice.

Le COSSI dispose d'une capacité d'inspection et d'audit pour évaluer la sécurité des systèmes d'information des services de l'Etat et aider les responsables à en améliorer le niveau. Cette capacité peut également être mobilisée dans le cadre du soutien et du contrôle qu'exerce l'Etat sur les opérateurs d'importance vitale.

L'ANSSI a également pour mission de **prévenir la menace**. Elle contribue pour cela 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'Etat, aux autorités publiques et aux autres acteurs de la conduite des situations d'urgence et des crises, des moyens sécurisés dont le fonctionnement doit être assuré en toutes circonstances. Avec l'appui du Centre de transmissions gouvernementales (CTG), elle met en œuvre les moyens gouvernementaux sécurisés de commandement et de liaison interministériels, parmi lesquels le réseau téléphonique RIMBAUD, qui permet la continuité de l'action gouvernementale et dessert les 300 plus hautes autorités gouvernementales parmi 4500 abonnés et l'Intranet sécurisé interministériel ISIS, seul réseau interministériel permettant, sur l'ensemble du territoire national, le passage en temps réel d'informations classifiées au niveau confidentiel-défense et outil de conduite de l'action gouvernementale en situation d'urgence ou de crise. ISIS met en relation 2000 décideurs publics.

Autre mission importante de l'agence, **l'ANSSI joue de plus en plus un rôle permanent d'assistance, de conseil et d'expertise en matière de sécurité des systèmes d'information au profit des administrations et des opérateurs d'importance vitale**. Elle exerce ainsi un rôle d'assistance à la maîtrise d'ouvrage des ministères et du secteur privé dès lors que la sécurisation de leurs systèmes d'information concerne les intérêts fondamentaux de la Nation. L'ANSSI apporte ainsi son soutien dans de nombreux projets d'importance (comme par exemple le passeport biométrique ou le dossier médical personnel) et elle œuvre à l'intégration de la sécurité des

systèmes d'information dans plusieurs programmes de défense (notamment les systèmes de communication ou de commandement) ou stratégiques (comme le système de positionnement par satellite Galileo). L'agence est également chargée de définir les recommandations générales, les référentiels techniques et les méthodes dans tous les aspects concourant à la sécurité des systèmes d'information.

L'ANSSI dispose aussi d'un **centre de formation à la sécurité des systèmes d'information** (CFSSI), qui dispense des enseignements spécialisés qui vont de la sensibilisation à la formation d'experts en cryptologie ou en systèmes. Chaque année, ce centre forme plus de 1 500 agents publics.

Enfin, l'agence développe **une politique de communication et de sensibilisation** afin d'informer régulièrement les entreprises et le grand public sur les menaces qui pèsent sur les systèmes d'information et sur les moyens de s'en protéger. Un portail de la sécurité informatique a ainsi été inauguré en 2008[1]. Il vise à offrir une information de qualité accessible au plus grand nombre.

En 2011, le gouvernement a décidé de **renforcer les prérogatives de l'ANSSI**. Par un décret du 11 février 2011, le Premier ministre a décidé de confier à l'agence la mission **d'autorité nationale** en matière de défense des systèmes d'information[2].

A ce titre, elle a la charge, en cas d'attaque informatique majeure contre la Nation, d'organiser la réponse et de décider des premières mesures urgentes à faire mettre en œuvre notamment par les administrations, par les opérateurs de communications électroniques et, à terme, par les opérateurs d'importance vitale.

Autrement dit, l'ANSSI pourrait décider, sur instruction des plus hautes autorités de l'Etat, le filtrage de certains protocoles ou le blocage de connexions à l'Internet, en cas de risque majeur contre la Nation.

2. La stratégie française en matière de cyberdéfense et de protection des systèmes d'information

Le 15 février 2011, l'ANSSI a rendu publique **la stratégie de la France en matière de défense et de sécurité des systèmes d'information**[3].

Cette stratégie repose sur **quatre objectifs** :

- faire de la France **une puissance mondiale de cyberdéfense** et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ;

---

[1] *http://www.securite-informatique.gouv.fr*

[2] *Décret n°2011-170 du 11 février 2011 modifiant le décret n°2009-834 du 7 juillet 2009*

[3] *Premier ministre, ANSSI, « Défense et sécurité des systèmes d'information – Stratégie de la France », février 2011*

Il s'agit d'assurer à notre pays des capacités autonomes et de prévoir une stratégie d'influence de manière à pouvoir peser sur ces questions à l'échelle internationale.

- garantir **la liberté de décision de la France** par la protection de l'information de souveraineté ;

Selon cet objectif, notre pays doit pouvoir protéger ses informations les plus confidentielles, ce qui suppose notamment une capacité autonome de production de produits de sécurité et des ressources humaines suffisantes dans certains domaines clés comme la cryptologie.

- renforcer **la cybersécurité des infrastructures vitales nationales** ;

Alors que traditionnellement la priorité était d'assurer la protection des informations de l'Etat, en particulier dans les domaines régaliens, comme les affaires étrangères ou la défense, cet objectif vise à prendre en compte les vulnérabilités existantes dans les secteurs d'importance vitale, comme l'énergie, les transports ou la santé.

- assurer **la sécurité dans le cyberespace**.

Il s'agit principalement par cet objectif de renforcer nos efforts en matière de lutte contre la cybercriminalité.

Le document propose également **sept axes** d'efforts :

- Mieux anticiper et analyser l'environnement afin de prendre les décisions les mieux adaptées ;

- Détecter les attaques et les contrer, alerter les victimes potentielles et les accompagner ;

- Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de préserver l'autonomie nécessaire ;

- Protéger les systèmes d'information de l'Etat et des opérateurs d'infrastructures vitales pour une meilleure résilience nationale ;

- Adapter notre droit afin de prendre en compte les évolutions technologiques et les nouveaux usages ;

- Développer nos collaborations internationales en matière de sécurité des systèmes d'information, de lutte contre la cybercriminalité et de cyberdéfense pour mieux protéger les systèmes d'information nationaux ;

- Communiquer, informer et convaincre afin de permettre aux Français de prendre la mesure des enjeux liés à la sécurité des systèmes d'information.

Cette stratégie s'accompagne d'une liste d'environ quarante orientations et actions concrètes à mettre en œuvre, qui n'ont pas été rendues publiques.

3. Le passage d'une posture de protection passive à une stratégie de cyberdéfense en profondeur

En réponse à la multiplication en France des attaques informatiques de grande ampleur, le gouvernement a décidé, le 25 mai 2011, d'accélérer **la montée en puissance du dispositif national de sécurité et de défense des systèmes d'information** en adoptant une série de mesures[1] :

- un **groupe d'intervention rapide** placé à l'ANSSI, formé d'experts capables d'intervenir sur les systèmes d'information de l'Etat et des opérateurs qui en feraient la demande, permettra de traiter dans les meilleurs délais les attaques les plus graves ;

Ce groupe d'intervention aura notamment pour mandat d'intervenir dans les administrations et les organismes publics ou encore chez les opérateurs critiques, notamment les opérateurs d'importance vitale, lorsque des indices laissent à penser qu'ils ont été l'objet d'une attaque informatique susceptible de présenter un danger pour la sécurité de leur activité, de menacer l'intégrité de leur patrimoine informationnel, de déséquilibrer le fonctionnement économique du pays ou de porter atteinte à la vie quotidienne des Français.

Dans le cas où une compromission grave serait découverte, le groupe d'intervention rapide devrait être en mesure, à la demande et en appui des équipes de l'administration, de l'entreprise et d'éventuels prestataires, 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, ce groupe d'intervention rapide devrait donner à la France une capacité d'assistance à nos alliés en cas de crise majeure de nature informatique.

- une **politique interministérielle de sécurité des systèmes d'information de l'Etat visant à homogénéiser et accroître la sécurité dans l'ensemble des ministères sera adoptée**.

L'objectif visé est d'élever et d'homogénéiser le niveau de sécurité de l'ensemble des systèmes d'information de l'Etat par la mise en œuvre de sécurités minimales communes. La mise en place généralisée de cartes à puce, qui présente de meilleures garanties que les simples mots de passe, devrait également améliorer significativement la sécurité des systèmes d'information de l'administration.

Dans ce cadre, **un réseau interministériel sécurisé (RIE)**, regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnent grave d'Internet, sera mis en place.

---

[1] *Compte rendu du Conseil des ministres du 25 mai 2011*

Aujourd'hui, chaque ministère dispose de son réseau informatique, avec des passerelles reliées à l'Internet. Il existe certes depuis 2007 un Intranet sécurisé interministériel, dénommé ISIS, mais celui-ci est réservé à l'information classifiée. Ce réseau permet l'échange et le partage de documents classifiés au titre du « confidentiel défense » entre acteurs gouvernementaux et remplace le traditionnel système de transport des plis « confidentiel défense » et « secret défense » par gendarme à motocyclette.

La construction d'un **réseau interministériel de l'Etat (RIE) protégé et résilient**, développé « à l'état de l'art », devrait assurer la continuité de l'action gouvernementale et administrative en cas de dysfonctionnement grave d'Internet, de limiter le nombre de passerelles d'interconnexion entre les administrations et l'Internet, qui sont autant de points de fragilité potentiels, et d'améliorer ainsi la détection des attaques au niveau des passerelles et notre capacité à y réagir. Accessoirement, un tel réseau permettrait de réduire les coûts de communications électroniques de l'Etat en réduisant le nombre de réseaux. Plusieurs pays, notamment l'Allemagne pour le gouvernement fédéral, disposent d'ores et déjà d'un tel réseau. Ce projet, qui représente un investissement de l'ordre de 70 millions d'euros par an, est sous la responsabilité de la direction interministérielle des systèmes d'information et de communication de l'Etat (DISIC), créée par le décret du 21 février 2012. D'après les informations recueillies par votre Rapporteur, le déploiement du RIE devrait commencer au printemps 2013 ;

- les **opérateurs publics et privés chargés d'infrastructures vitales** seront invités à participer avec l'Etat à **un partenariat** visant à renforcer la défense et la sécurité de leurs systèmes d'information ;

Ce partenariat entre l'Etat et les opérateurs d'infrastructures critiques doit notamment permettre d'améliorer la sensibilisation des opérateurs à la sécurité des systèmes d'information, de mieux connaître les faiblesses de leurs systèmes d'information, de prévenir les attaques sur les systèmes critiques et de définir les chaînes de compétence et de responsabilité en matière de sécurité des systèmes d'information.

Cela passe notamment par le développement des échanges d'information entre l'Etat et les opérateurs critiques, le partage et l'analyse des remontées d'incidents, ainsi que les audits de sécurité, et par la création d'un réseau d'alerte en cas d'attaque informatique.

- la **sécurité des systèmes d'information sera incluse dans les formations supérieures**, en commençant par les formations scientifiques et techniques, afin que l'ensemble des étudiants acquièrent un socle commun de connaissances et de bonnes pratiques en ce domaine ;

- un **centre de recherche** associant l'Etat et les entreprises sera créé afin d'optimiser les capacités de recherche existantes et de soutenir des projets structurants.

4. Les mesures prises par les différents ministères : l'exemple du ministère de la défense

La création de l'ANSSI a modifié sensiblement le paysage institutionnel français de la sécurité des systèmes d'information.

Si le Secrétaire général de la défense et de la sécurité nationale reste chargé, au nom du Premier ministre, du pilotage de la politique nationale en matière de sécurité des systèmes d'information, il s'appuie désormais sur l'Agence nationale de la sécurité des systèmes d'information. Afin de préparer la stratégie nationale, un comité stratégique de la SSI a également été institué par le décret portant création de l'ANSSI.

Enfin, conformément aux recommandations du Livre blanc de 2008, il a été décidé, en complément de la création de l'ANSSI, la mise en place au niveau de chaque zone de défense et de sécurité, d'un observatoire zonal de la sécurité des systèmes d'information (OzSSI). Ces observatoires, créés par le ministère de l'Intérieur, ont pour mission de relayer, sur l'ensemble du territoire national, les mesures prises pour améliorer la sécurité des systèmes d'information.

Outre le SGDSN et l'ANSSI, **plusieurs ministères disposent de compétences spécifiques** intéressant la sécurité des systèmes d'information : le **ministère de la défense**, avec la direction générale de l'armement, au travers de son expertise technique, et **les services de renseignement** (Direction générale de la sécurité extérieure – DGSE - et Direction de la protection et de la sécurité de la défense - DPSD) ; **le ministère de l'intérieur**, avec la Direction centrale du renseignement intérieur (DCRI), l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et les services spécialisés de la gendarmerie nationale, en particulier le département « cybercriminalité » du service technique de recherche judiciaire et de documentation (STRJD) et le département informatique et électronique de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), ou encore les ministères de l'économie, des finances et du budget.

Enfin, **chaque ministère reste responsable de la sécurité de ses propres systèmes d'information**. L'organisation repose sur les hauts fonctionnaires de défense et de sécurité (HFDS), placés auprès de chaque ministre, éventuellement assistés d'un fonctionnaire de sécurité des systèmes d'information (FSSI), qui est chargé d'animer la politique de sécurité des systèmes d'information. Chaque ministre désigne en outre des autorités qualifiées en sécurité des systèmes d'information (AQSSI), qui sont responsables de la sécurité des systèmes d'information au sein de leur périmètre. Aux différents échelons des administrations centrales et des services déconcentrés sont généralement désignés des responsables de la sécurité des systèmes d'information (RSSI).

A la suite des préconisations du Livre blanc, **des outils informatiques spécialisés ont été déployés dans plusieurs ministères afin de permettre de déceler les signes d'attaques informatiques.**

Votre rapporteur a souhaité consacrer une place particulière au **ministère de la défense et aux armées.** Le ministère de la défense a, en effet, réformé récemment son organisation afin de l'adapter à une stratégie de « cyberdéfense en profondeur ».

Par ailleurs, si l'ANSSI est autorité nationale de défense, le ministère de la défense et les forces armées conservent un rôle particulier dans ce domaine, notamment en raison des opérations et des missions à caractère militaire conduites sous l'autorité du chef des armées et dont le cadre d'action ne se limite pas aux zones sous souveraineté nationale.

L'organisation au sein du ministère de la défense et des armées, qui a été réformée récemment par une instruction ministérielle de janvier 2012, repose sur **une distinction entre la protection et la défense des systèmes d'information**. En effet, même si la protection et la défense des systèmes d'information sont complémentaires et mettent en œuvre plusieurs concepts et moyens communs, elles font intervenir des cycles temporels bien différents, la première planifiant ses actions à moyen et long terme, là où la seconde agit en temps réel. Elles peuvent par conséquent être traitées par des chaînes distinctes.

C'est le cas au ministère de la défense, où la partie « protection » est animée par le fonctionnaire de sécurité des systèmes d'information (FSSI) et la partie « défense » est commandée par un officier général à la cyberdéfense (OG CYBER).

La **protection** des systèmes d'information recouvre l'ensemble des moyens et des méthodes mis en place pour protéger l'information, les systèmes informatiques et les réseaux de communication par des moyens techniques (cryptographie, analyse et filtrage de flux, anti-virus, etc.) et organisationnels (sensibilisation, formation, surveillance). Elle aboutit, via un processus d'homologation, à la délivrance d'une aptitude à opérer en sécurité, aptitude qu'il convient ensuite d'entretenir par un processus de maintien en condition de sécurité tout au long de la vie du système. Elle repose sur une chaîne mise en place par cinq autorités qualifiées (AQSSI) et animée par un fonctionnaire de sécurité des systèmes d'information (FSSI), rendant compte au haut fonctionnaire correspondant de défense et de sécurité (HFCDS), qui est le chef du cabinet militaire du ministre de la défense

Les cinq autorités qualifiées (AQSSI) sont le chef d'état major des armées, le directeur général de la sécurité extérieure, le directeur de la protection et de la sécurité de la défense, le secrétaire général de l'administration et le délégué général pour l'armement. Ces cinq autorités qualifiées rendent compte au ministre et désignent un représentant qui travaille en étroite concertation avec le fonctionnaire de la sécurité des systèmes d'information (FSSI), placé au sein de la direction générale des systèmes

d'information et de communication du ministère de la défense (DGSIC). Créée en 2006 et placée directement auprès du ministre de la défense, la DGSIC joue un rôle d'animation, d'expertise et de conseil en matière de systèmes d'information et de communication. Elle dispose d'une sous-direction de la sécurité des systèmes d'information. La direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) est, pour sa part, l'opérateur principal des systèmes d'information et de communication du ministère de la défense.

La chaîne fonctionnelle de sécurité des systèmes d'information du ministère de la défense a été réformée récemment, avec le regroupement, sous l'autorité du chef d'Etat major des armées, des chaînes d'armées, de façon à suivre la mise en place des bases de défense. L'organisation distingue mieux désormais le rôle des responsables de la sécurité des systèmes d'information (RSSI) dévolus à des projets ou des programmes de systèmes d'information et de communication, et les fonctions d'officier de la sécurité des systèmes d'information (OSSI), qui ont en charge le volet organisationnel de la cyberprotection. Au total, il existe environ un millier d'agents de la sécurité des systèmes d'information au sein du ministère de la défense et le coût total de la cybersécurité est évalué à environ 44 millions d'euros par an.

La **défense** des systèmes d'information, qui vise à garantir en temps réel la sécurité et la disponibilité des systèmes d'information contre les attaques informatiques, en complétant les moyens de protection par des mesures réactives et une capacité de gestion de crise, traitant à la fois de la reconfiguration du système d'information et des missions ou priorités des organismes attaqués, relève du chef d'état-major des armées.

Une structure particulière, intégrée à la chaîne de planification et de conduite des opérations, a été mise en place en juillet 2011 sous le commandement d'un officier général, **l'officier général à la cyberdéfense**. Il ne s'agit pas d'une nouvelle division, mais d'une cellule légère de commandement, de coordination et d'animation, qui ne comporte que quelques militaires, mais qui est à la tête d'un ensemble de correspondants et qui entretient des relations étroites, tant avec la chaîne chargée de la sécurité des systèmes d'information, qu'avec l'ANSSI[1].

Le **centre d'analyse en lutte informatique défensive** (CALID), placé sous l'autorité de l'officier général à la cyberdéfense, est chargé de contribuer à la préparation et de la conduite des opérations de cyberdéfense sur les réseaux et systèmes du ministère de la défense. Il dispose d'outils centralisés de surveillance des réseaux et intervient en cas d'incident ou d'attaque informatique. Le CALID compte actuellement une vingtaine de militaires, ce qui ne lui permet pas encore d'être opérationnel 24 heures sur 24, 7 jours sur 7. A titre de comparaisons, la structure équivalente au Royaume-Uni dispose de plus de 80 agents, soit quatre fois plus.

[1] *Un protocole de coopération a d'ailleurs été signé entre l'ANSSI et l'état-major des armées*

Le CALID travaille en collaboration avec le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI. Les deux centres devraient être colocalisés au second semestre 2013, ce qui permettra de renforcer la coopération et les synergies entre les deux entités.

Le ministère de la défense et les armées se sont dotés d'**un concept et d'une doctrine interarmées de cyberdéfense**, documents adoptés respectivement en juillet 2011 et en janvier 2012, mais qui n'ont pas été rendus publics.

A l'image de ce qui existe dans les armées pour les différents milieux (air, terre, mer), il existe donc au sein du ministère de la défense et des armées une chaîne qui prépare et une autre chaîne qui est chargée de l'opérationnel.

La **direction générale de l'armement** (DGA) joue également un rôle important. Elle est chargée de la maîtrise d'ouvrage des systèmes d'armes, des systèmes d'information à usage militaire, mais aussi de produits de haut niveau de sécurité pour les besoins militaires et les besoins interministériels, à l'image du téléphone cellulaire chiffrant Teorem ou du chiffreur Echinops, qui permet de sécuriser les flux des réseaux les plus sensibles, comme les communications du porte-avions Charles de Gaulle. Le centre maîtrise de l'information de la DGA, situé à Bruz, à proximité de Rennes, dispose d'environ 150 experts de haut niveau.

En définitive**, le ministère de la défense a su adapter son organisation en matière de sécurité et de défense des systèmes d'information**, de manière à ce que cette dimension soit pleinement prise en compte dans la chaîne opérationnelle.

Toutefois, il n'en va pas de même dans tous les autres ministères.

C. NOTRE DISPOSITIF CONNAÎT ENCORE D'IMPORTANTES LACUNES

En dépit des progrès incontestables accomplis depuis le Livre blanc de 2008, **la situation de la France au regard de la menace provenant des attaques informatiques reste encore insatisfaisante**.

Malgré un réel effort de rattrapage, notre pays accuse encore un important retard concernant les moyens et les effectifs de l'agence chargée de la sécurité des systèmes d'information, par rapport à ceux dont disposent les services homologues en Allemagne ou au Royaume-Uni.

Si l'ANSSI dispose du statut d'une agence interministérielle et d'autorité de sécurité et de défense, en pratique, **les textes ne lui reconnaissent pas l'autorité nécessaire pour assurer l'application uniforme, au sein des administrations, des règles inhérentes à la sécurité des systèmes d'information**. Au sein des administrations elles mêmes, les avis émis par les responsables de la sécurité des systèmes d'information semblent être pris en compte de manière très aléatoire.

Elle ne dispose **pas non plus des moyens nécessaires pour donner une plus large diffusion aux actions de sensibilisation, de formation ou de conseil**, **ni pour mener à l'échelle souhaitable les activités d'audit et d'inspection** auprès des administrations ou des opérateurs d'importance vitale.

Surtout, **la synergie entre acteurs publics et privés, qu'il s'agisse des entreprises ou des opérateurs d'importance vitale, reste très insuffisante,** alors qu'un partenariat étroit serait indispensable.

1. Les effectifs et les moyens de l'ANSSI restent limités par rapport à ceux dont disposent nos principaux partenaires

L'ANSSI a connu ces dernières années une augmentation significative de ses effectifs et de ses moyens. D'un effectif de 120 agents lors de sa création, en 2009, elle comptait 170 agents en février 2011 et elle devrait atteindre 250 personnes d'ici la fin de l'année 2012.

Si l'on peut se féliciter de cet effort important, il convient toutefois de souligner qu'il s'agit là davantage **d'un rattrapage nécessaire**, la France ayant pris beaucoup de retard par le passé par rapport à d'autres pays.

Pour accroître sa capacité d'intervention et de soutien, le gouvernement de M. François Fillon a d'ailleurs décidé, en mai 2011, d'accélérer l'augmentation des effectifs et des moyens de l'ANSSI, afin de porter ses effectifs à 360 d'ici 2013, ce dont on peut se féliciter.

Mais, même après ce renforcement, **les effectifs et les moyens de l'ANSSI resteront encore très inférieurs à ceux dont disposent les services homologues au Royaume-Uni ou en Allemagne, qui sont de l'ordre de 500 à 700 agents, soit deux fois plus**.

De plus, si le budget de l'ANSSI est passé de 45 millions d'euros en 2009 à **75 millions d'euros** en 2012, **il reste encore loin de l'objectif affiché de 90 millions d'euros**. Au sein de ce budget, les dépenses de fonctionnement et d'investissements ont été multipliées par deux en quatre ans, passant de 24 millions d'euros en 2009 à 55,8 millions d'euros en 2012, et les crédits de personnels sont de l'ordre de 20 millions d'euros.

2. La sécurité des systèmes d'information n'est pas toujours considérée comme une priorité par les différents ministères

Si certains ministères, comme le ministère de la défense, ont pris des mesures pour renforcer la protection de leurs systèmes d'information, beaucoup de ministères demeurent encore peu sensibilisés aux menaces liées aux attaques contre les systèmes d'information.

Selon les informations recueillies par votre rapporteur, dans de nombreux ministères, le renforcement de la sécurité des systèmes d'information n'est clairement pas une priorité et relève de la procrastination.

Ainsi, pour ne citer qu'un seul exemple, il ne sert à rien de classifier ou de chiffrer une note confidentielle ou un télégramme diplomatique si le contenu de cette note ou de ce télégramme se retrouve dans un courriel envoyé par l'Internet.

Peu de ministères disposent d'une véritable politique de sécurité des systèmes d'information. Bien souvent les systèmes informatiques utilisés par les administrations sont considérés comme immarcescibles, alors qu'ils présentent en réalité de nombreuses vulnérabilités.

Les fonctionnaires de la sécurité des systèmes d'information occupent en règle générale une place modeste dans la hiérarchie et ne parviennent pas à faire entendre leur voix, face aux directeurs des systèmes d'information ou aux responsables des différentes directions sectorielles, ignorant la réglementation, peu conscients des risques et soucieux avant tout de disposer à moindre coût d'outils informatiques efficaces et ergonomiques.

La sécurité informatique est souvent perçue par les responsables et les utilisateurs comme une contrainte inutile et coûteuse. Elle n'est pas suffisamment prise en compte dans les projets informatiques des ministères, qui ont tendance à minorer l'importance de cette question et à ne pas prendre en considération les avis des responsables de la sécurité des systèmes d'information.

Ainsi, comme cela a été confirmé à votre rapporteur, de nombreux ministères ne connaissent même pas la cartographie de leurs propres réseaux et ignorent souvent la finalité de leurs propres systèmes d'information.

Or, comment peut-on prétendre assurer une protection de ses systèmes informatiques, si l'on ne sait même pas localiser précisément l'un de ses ordinateurs qui a été infecté à la suite d'une attaque informatique ou si l'on ignore à quoi sert son serveur informatique ?

Afin de renforcer la sensibilisation des ministères, le précédent gouvernement a choisi de rendre publique l'attaque informatique massive dont a fait l'objet le ministère de l'économie et des finances découverte à la veille de la présidence française du G8 et du G20, et il convient de s'en féliciter.

Cette affaire ne représente cependant que « la pointe de l'iceberg », et il conviendrait, aux yeux de votre rapporteur, de poser le principe qu'à l'avenir l'ensemble des attaques informatiques contre les systèmes d'information de l'Etat devraient, sous réserve de quelques exceptions et une fois qu'elles auront été traitées, être rendues publiques.

3. Les entreprises et les opérateurs d'importance vitale demeurent encore insuffisamment sensibilisés à la menace

De manière générale, **les entreprises françaises, et notamment les PME, ne semblent pas encore avoir pris en compte la réalité de la menace liée aux attaques contre les systèmes d'information.**

Ce constat dressé par le rapport Lasbordes en 2006 reste encore largement d'actualité.

Traditionnellement peu sensibilisées aux enjeux soulevés par l'intelligence économique, notamment par rapport aux entreprises anglo-saxonnes, les entreprises françaises ne paraissent pas accorder une attention suffisante à cette question.

En dehors de quelques grands groupes, on constate un manque d'implication de la direction de l'entreprise, une sensibilisation et une formation insuffisante des personnels, une absence de stratégie en matière de protection des systèmes d'information, et des lacunes en matière d'identification pertinente des systèmes ou des données sensibles de l'entreprise, une insuffisance des budgets dédiés à la sécurité des systèmes d'information.

Ainsi, d'après le dernier rapport[1] réalisé par le Club de la sécurité de l'informatique français (CLUSIF), consacré aux menaces informatiques, fondé sur une enquête auprès de 350 entreprises, près de 80 % des entreprises interrogées ne mesurent pas régulièrement leur niveau de sécurité lié à l'information, 46 % ne disposent pas d'un responsable de la sécurité des systèmes d'information et seulement 53 % d'entre-elles ont mis en place une cellule dédiée à la gestion des incidents de sécurité.

En particulier, les PME ne disposent souvent pas des ressources nécessaires pour investir dans la sécurité des systèmes d'information, ni de personnels formés et compétents dans ce domaine.

Or, face à l'espionnage informatique, la problématique de la sécurité des systèmes d'information des entreprises – et notamment de celles des secteurs jugés stratégiques – représente un enjeu majeur.

A l'image d'AREVA, un grand nombre d'entreprises françaises auraient été victimes ces dernières années de l'espionnage informatique. Ainsi, selon une étude de Symantec, fondée sur des enquêtes directes, 70 % des entreprises françaises auraient été victimes d'une attaque informatique en 2010, chiffre comparable à la moyenne mondiale mais à prendre toutefois avec précaution.

En effet, les responsables de ces entreprises ont toujours été d'une très grande discrétion, par crainte notamment de mettre en péril les résultats économiques, le cours en bourse ou encore l'image de leur entreprise.

---

[1] *CLUSIF, les « Menaces Informatiques et Pratiques de Sécurité en France », édition 2012*

Enfin, reste la question centrale des **opérateurs d'importance vitale**.

Il n'existe pas de définition communément admise au niveau international de ces opérateurs.

La Commission européenne propose la définition suivante[1] : *« les infrastructures critiques sont des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des Etats membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base ».*

Dans le cas de la France, douze secteurs d'importance vitale ont été identifiés, regroupant environ deux cents trente opérateurs ou entreprises, issus du secteur public ou du secteur privé.

Indispensables au bon fonctionnement du pays, **les opérateurs d'importance vitale représentent aujourd'hui des cibles particulièrement vulnérables aux attaques informatiques.**

Ainsi, la découverte du ver informatique STUXNET en juin 2010 a montré qu'un code informatique malveillant pouvait porter atteinte à des infrastructures critiques totalement isolées d'Internet.

Or, ces attaques, si elles devaient réussir, pourraient avoir des conséquences très graves.

Quel serait le moyen le plus simple de provoquer une perturbation majeure d'un pays ?

Un moyen très simple serait de s'en prendre à la distribution d'électricité, aux réseaux de transport ou bien encore aux hôpitaux. Déjà le ver informatique *Conficker* avait attiré l'attention sur la vulnérabilité de nombreux équipements biomédicaux installés dans les hôpitaux.

La principale difficulté tient cependant à la très grande diversité des opérateurs d'importance vitale.

On constate, en effet, de fortes différences entre les secteurs concernés, qu'il s'agisse de l'existence ou non d'une autorité de régulation, en termes de réglementation ou encore de relations avec la puissance publique.

Ainsi, dans certains secteurs, à l'image du secteur bancaire, de l'aviation civile ou encore de l'énergie nucléaire, les préoccupations de sécurité ne sont pas absentes et l'autorité de régulation joue un rôle important.

Mais il n'en va pas de même dans tous les secteurs.

---

[1] *Communication de la Commission européenne sur la « protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme », d'octobre 2004*

Or, l'ANSSI n'a pas les moyens d'assurer la protection de tous les opérateurs d'importance vitale et il est donc indispensable d'encourager les opérateurs, sur une base sectorielle, à renforcer les mesures de protection de leurs systèmes d'information.

De nombreux pays, à l'image des Etats-Unis ou de l'Allemagne, ont fait de la protection des infrastructures d'importance vitale une priorité nationale.

A titre d'exemple, Israël a créé une agence spécialement dédiée à la protection des systèmes d'information d'opérateurs critiques (NISA), qui dispose de pouvoirs d'intervention étendus, qui vont de l'assistance lors de la conception des systèmes à la détection et au traitement des incidents, et d'effectifs importants, puisque cette agence compte environ 140 personnes. Une vingtaine de secteurs ont été identifiés et il existe des relations suivies avec chacun des opérateurs.

Or, **dans ce domaine**, la France accuse encore **un réel retard par rapport à nos principaux alliés et partenaires.**

Comme cela a été confirmé par l'ensemble de ses interlocuteurs, les échanges entre l'ANSSI et les opérateurs d'importance vitale sont très limités et on constate une méconnaissance réciproque.

Ensuite, en raison de leur diversité, la protection des systèmes d'information n'est clairement pas une priorité pour la plupart de ces opérateurs.

Surtout, la plupart des opérateurs d'importance vitale ne sont pas organisés pour répondre efficacement à un grave incident informatique et l'ANSSI n'a pas les moyens de faire face à une crise générale paralysant un secteur entier du pays.

Enfin, à la différence de certains pays comme le Royaume-Uni, **la France ne dispose pas de capacités de protection et de systèmes permanents de détection des attaques informatiques à l'entrée des réseaux des opérateurs d'importance vitale**.

De ce fait, l'Etat et les opérateurs eux-mêmes ignorent le plus souvent les attaques informatiques dont font l'objet les infrastructures vitales de notre pays.

Pour votre rapporteur, **l'insuffisante sécurité des systèmes d'information des opérateurs d'importance vitale constitue aujourd'hui la principale lacune du dispositif français et un véritable** *« Talon d'Achille »***.**

Il est donc indispensable de faire de cette question une priorité nationale.

IV. FAIRE DE LA PROTECTION ET DE LA DÉFENSE DES SYSTÈMES D'INFORMATION UNE VÉRITABLE PRIORITÉ NATIONALE ET EUROPÉENNE

Si depuis le Livre blanc sur la défense et la sécurité nationale de 2008 des avancées importantes ont été réalisées par la France pour renforcer la sécurité des systèmes d'information, notre pays n'a sans doute pas encore pris toute la mesure de l'ampleur des risques et des enjeux soulevés par les attaques informatiques, qui revêtent désormais une dimension stratégique.

Dans ce contexte, l'élaboration du nouveau Livre blanc, ainsi que la rédaction de la future Loi de programmation militaire, représentent de réelles opportunités pour renforcer la prise de conscience et l'efficacité des réponses face à ces menaces majeures pour notre défense et notre sécurité, tant au niveau national, qu'à l'échelle européenne.

Votre rapporteur estime que **la protection et la défense des systèmes d'information** devrait être érigée en **véritable priorité nationale**, portée **au plus haut niveau de l'Etat**, et faire l'objet d'**une stratégie et d'une action plus résolue** de **l'Union européenne**.

A. LA NÉCESSITÉ D'UNE FORTE MOBILISATION AU SEIN DE L'ETAT

Le renforcement de la protection et de la défense des systèmes d'information devrait d'abord faire l'objet d'une **plus forte mobilisation au sein de l'Etat.** Votre rapporteur considère qu'il faudrait agir sur **trois** principaux leviers : **le renforcement des effectifs et des moyens**, de manière à les porter à la hauteur de ceux dont disposent nos principaux partenaires européens ; **un important effort de sensibilisation et la mise en place de mesures de protection** au sein des différentes administrations, et, enfin, **le développement de « capacités offensives »**, car on ne peut se défendre efficacement que si l'on connaît les modes d'attaques.

1. Renforcer les effectifs et les prérogatives de l'ANSSI afin de les porter à la hauteur de ceux dont disposent nos principaux partenaires européens

La création de l'ANSSI a permis de doter notre pays d'une structure centrale en charge de la sécurité des systèmes d'information et d'un interlocuteur unique pour les administrations et les entreprises.

Comme votre rapporteur a pu le constater lors de ses entretiens en France comme à l'étranger, **l'ANSSI dispose d'une compétence et d'une expertise reconnue** en matière de protection des systèmes d'information et l'ensemble des personnalités rencontrées, notamment les responsables publics ou privés ayant eu à gérer des attaques informatiques massives, ont loué les très grandes qualités de ses personnels et de son directeur général.

Ayant pu comparer lors de ses déplacements, le dispositif français avec les différents modèles étrangers, notamment aux Etats-Unis, au Royaume-Uni ou en Allemagne, votre rapporteur a également pu constater **la pertinence de ce dispositif**, qui paraît le mieux correspondre à l'organisation administrative et à la culture de notre pays.

Le **modèle français** se caractérise, en effet, par **son caractère centralisé et interministériel** et **par une stricte séparation entre les aspects préventifs et défensifs**, confiés à l'ANSSI, **et les aspects offensifs**, qui relèvent des armées et des services spécialisés.

Réunir dans les mêmes mains les aspects défensifs et le volet offensif, à l'image des Etats-Unis ou du Royaume-Uni, ne parait pas opportun, car cela éloignerait l'agence des entreprises et des opérateurs d'importance vitale, les entreprises françaises n'ayant pas la même sensibilité à l'intelligence économique et au renseignement que leurs homologues dans les pays anglo-saxons.

Pour sa part, le caractère interministériel de l'agence, qui découle de son rattachement au Premier ministre, lui confère une légitimité que beaucoup de nos partenaires étrangers nous envient.

Aux côtés de l'agence, d'autres acteurs continuent, en effet, de jouer un rôle important, qu'il s'agisse des armées et du ministère de la défense, à travers son expertise propre, du ministère de l'économie et des finances, pour le développement de l'administration électronique, du ministère du redressement productif pour le soutien aux entreprises, ou des services de renseignement, qui disposent d'équipements techniques et de personnels spécialisés.

Aux yeux de votre rapporteur, la coordination, nécessaire pour veiller à la cohérence des actions et des moyens, ne peut **relever que de l'autorité du Premier ministre**, à qui il appartient de définir les axes stratégiques, de suivre leur mise en œuvre et de veiller à la bonne répartition des moyens humains, techniques et financiers.

Le rattachement de l'ANSSI au Secrétaire général de la défense et de la sécurité nationale, plutôt que directement au Premier ministre ou aux services du Premier ministre, semble également devoir être conservé, du moins dans un proche avenir, car s'il présente certains inconvénients, notamment du point de vue des relations avec les entreprises et de la diffusion des informations hors du cercle de la défense et de la sécurité nationale, il a aussi des avantages certains, en particulier en ce qui concerne le poids de l'agence à l'égard des autres ministères.

On peut également s'interroger sur **le statut juridique actuel de l'ANSSI**. Le statut de l'ANSSI repose actuellement sur un simple décret. Ne serait-il pas utile de renforcer son statut en lui conférant une base législative, dans le cadre d'une loi générale relative à la protection des systèmes d'information ?

La principale faiblesse de l'agence tient cependant à **la modestie de ses effectifs et de ses moyens.**

Comme on l'a vu précédemment l'ANSSI a connu ces dernières années une augmentation significative de ses personnels, mais **le nombre total de ses agents reste encore inférieur de moitié, voire d'un tiers, à celui des agences homologues de nos partenaires britanniques ou allemands.**

Même si l'on ne peut pas négliger les difficultés à recruter un nombre aussi significatif de personnels spécialisés dans des délais aussi courts, il semble souhaitable que le prochain Livre blanc fixe des objectifs ambitieux.

Pour votre rapporteur, cet objectif doit être de **parvenir progressivement, sur plusieurs années, à un niveau similaire à celui des services équivalents de l'Allemagne et du Royaume-Uni**.

Il semble donc souhaitable d'élaborer, dans le cadre du nouveau Livre blanc, un **plan pluriannuel** permettant de poursuivre au même rythme, voire d'amplifier, l'augmentation des effectifs de l'ANSSI dans les prochaines années et de renforcer parallèlement l'effort d'investissement.

Une croissance régulière des effectifs de l'ANSSI de l'ordre de 80 personnes supplémentaires par an lui permettrait ainsi d'atteindre 500 personnes à la fin de l'année 2015. Les volumes d'effectifs et d'investissements concernés sont au demeurant modestes.

Une telle augmentation des effectifs de l'ANSSI permettrait notamment :

- d'armer en personnels le **centre de surveillance et de détection,** le **centre opérationnel et le groupe d'intervention rapide** afin de renforcer les capacités de l'agence en matière de détection des attaques informatiques et de réponse ;

- de poursuivre et d'**accélérer le déploiement des réseaux de communication sécurisés ;**

- de poursuivre et d'accélérer **le développement et l'acquisition de produits hautement sécurisés** directement liés à la protection de l'Etat, notamment en matière de moyens de mobilité ;

- de doter l'agence des moyens de **développer la politique de labellisation de produits et services**, en vue de plus largement diffuser ces produits au sein des administrations et du secteur privé ;

- de soutenir les services informatiques des administrations dans **l'intégration des produits et services sécurisés**, ainsi que dans l'intégration des produits agréés et qualifiés et de systèmes d'exploitation durcis ;

- de constituer au sein de l'agence le **réservoir de compétences** ; il permettrait de regrouper et de capitaliser l'expertise en vue de la mettre à disposition des administrations ou des opérateurs d'importance vitale lors de la conception de leurs systèmes d'information ;

- de **renforcer les capacités en matière d'audit, d'inspection et de réalisation de tests d'intrusion**, **ainsi que de conseil au secteur privé** ;

- d'**accentuer les programmes de formation** et d'élargir le public visé notamment au secteur privé. Il serait notamment utile de créer un centre d'entraînement où les informaticiens du secteur public et du secteur privé pourraient être confrontés à la réalité d'une attaque informatique ;

- de **permettre à l'agence de mener une politique de communication** destinée à renforcer la sensibilisation des responsables des administrations et des entreprises, ainsi que des utilisateurs.

Ce plan devrait s'accompagner de l'instauration d'une **politique de ressources humaines** au sein des services de l'Etat concernant les spécialistes de la sécurité informatique, en encourageant le recrutement, la formation, les mobilités et le déroulement des carrières au sein et entre les différents services de l'Etat.

S'agissant des **prérogatives de l'ANSSI**, elles mériteraient d'être **sensiblement renforcées.**

En effet, **ces prérogatives ne sauraient se limiter à de simples recommandations laissées à la libre appréciation des administrations**, comme c'est malheureusement le cas actuellement, mais elles devraient être dotées d'une force juridiquement contraignante à l'égard des administrations, pour permettre une mise en œuvre effective des prescriptions touchant à la sécurité de systèmes d'information. Ce renforcement des prérogatives de l'agence est d'ailleurs consubstantiel à son rôle d'autorité nationale en matière de sécurité et de défense des systèmes d'information.

L'ANSSI devrait ainsi être en mesure :

- dans l'attente de l'édification du Réseau interministériel de l'Etat, d'**imposer aux administrations une réduction du nombre de leurs passerelles vers l'internet**, et **développer les systèmes de surveillance de ces passerelles permettant de détecter les attaques** ;

- de **désigner les produits de haute sécurité que les administrations devront obligatoirement utiliser pour les réseaux les plus sensibles** ;

- d'édicter des prescriptions de sécurité **pour les autres réseaux sensibles des administrations**, et de s'assurer, par une procédure de validation, que les solutions retenues par l'administration concernée s'y sont bien conformées ;

- de veiller, dans le cadre de ces prescriptions et de cette procédure de validation applicable aux **réseaux sensibles des administrations**, au **recours systématique à des produits labellisés,** de manière à soutenir l'offre de ces produits et à les rendre ainsi plus accessibles sur le marché ;

- de soutenir les services informatiques des administrations dans **l'intégration de ces produits**, ainsi que **dans l'intégration des produits agréés et qualifiés et de systèmes d'exploitation durcis** ;

- de rendre **obligatoire** l'adoption par les administrations, pour leurs réseaux sensibles, ainsi que par les opérateurs d'importance vitale, de **dispositifs garantissant la continuité du service en cas d'attaque majeure**, sous la forme par exemple de systèmes redondants ;

- de rendre **obligatoire** l'application de la politique interministérielle de sécurité des systèmes d'information et de disposer d'**un pouvoir de validation** des politiques de sécurité ministérielles complémentaires et des grands projets sensibles **;**

- de **rendre obligatoire la mise en œuvre de ses préconisations** à la suite des audits, des exercices ou des tests ;

- d'**étendre ses missions d'inspection et la réalisation des tests d'intrusion aux opérateurs d'importance vitale**.

2. Donner plus de force à la protection et à la défense des systèmes d'information au sein de chaque ministère

Si la France dispose avec l'ANSSI et la stratégie nationale d'outils importants en matière de cyberdéfense, il n'en demeure pas moins que **les ministères restent encore diversement sensibilisés à la menace** que représentent les attaques informatiques.

Il existe certes au sein de chaque ministère un fonctionnaire de la sécurité des systèmes d'information. Mais on constate souvent que celui-ci n'occupe qu'une faible place hiérarchique au sein de l'organigramme du ministère et surtout qu'il ne parvient pas à imposer aux différentes directions sectorielles et aux directeurs des systèmes d'information une prise en compte suffisante des préoccupations liées à la sécurité des systèmes d'information. Pour sa part, le haut fonctionnaire de défense et de sécurité, fonction souvent cumulée par le secrétaire général du ministère, ne peut se consacrer entièrement à cette tâche.

Pour votre Rapporteur, **la protection des systèmes d'information doit devenir une véritable priorité prise en compte dans l'action de chaque ministère.** Chaque ministère devrait disposer d'une **politique en matière de sécurité des systèmes d'information**. Celle-ci devra décliner et s'appuyer sur la politique de sécurité des systèmes d'information de l'Etat, à vocation interministérielle, actuellement en cours d'élaboration par l'ANSSI.

De la même manière qu'au niveau interministériel il a été décidé de créer une autorité nationale, l'ANSSI, avec des prérogatives étendues, il paraît nécessaire de **rehausser le statut des fonctionnaires de la sécurité des systèmes d'information** et de renforcer leurs prérogatives par rapport aux responsables des différentes directions et notamment par rapport au directeur

des systèmes informatiques, afin qu'ils deviennent de véritables directeurs, voire même des secrétaires généraux, chargés de la sécurité et de la défense des systèmes d'information, auxquels devront être soumis pour avis les projets informatiques des administrations.

Ainsi, dans le cas du ministère de la défense, une instruction ministérielle permet au fonctionnaire de la sécurité des systèmes d'information de solliciter ponctuellement l'avis de la direction générale de l'armement pour analyser la sécurité d'un système d'information d'un projet en cours d'élaboration. Il semblerait utile de s'en inspirer afin que les fonctionnaires de la sécurité des systèmes d'information puissent solliciter une expertise, en interne ou auprès de l'ANSSI, concernant la sécurité des systèmes d'information des projets informatiques de leur administration.

Il pourrait également être utile de renforcer, sous l'égide du ministère de l'intérieur, au niveau de chaque zone de défense et de sécurité, la mission et les moyens des **observatoires zonaux de la sécurité des systèmes d'information** (OzSSi), qui jouent un rôle important de relais vers l'administration territoriale et hospitalière, les collectivités locales, les opérateurs d'importance vitale au niveau local, ainsi que les acteurs industriels.

La **direction interministérielle des systèmes d'information et de communication de l'Etat** (DISIC), qui est saisie par les différentes administrations de tout projet informatique dont le coût dépasse un certain montant, ne compte actuellement que 3 spécialistes en matière de sécurité des systèmes d'information sur un effectif total d'une vingtaine d'agents. Elle devrait voir ses effectifs et ses moyens renforcés, et développer ses échanges avec l'ANSSI afin d'assurer la prise en compte, le plus en amont possible, de la sécurité des systèmes d'information dans les projets informatiques des ministères. Ainsi, on peut se demander s'il ne serait pas opportun que la DISIC donne un avis négatif à tout projet informatique important ne disposant pas d'une stratégie d'homologation en matière de sécurité informatique.

C'est notamment ce qui a été prévu récemment au ministère de la défense et pour les armées, où, pour éviter une pratique courante de l'administration consistant à minimiser *a priori* les besoins de sécurité des projets pour éviter d'avoir à appliquer la réglementation relative la sécurité des systèmes d'informations et de communication, il a été décidé que tout système informatique du ministère devrait dorénavant faire l'objet d'une homologation. Pourquoi ne pas réserver aussi un pourcentage significatif du montant des projets informatiques (de l'ordre de 10% du budget informatique pour un projet standard, hors anti-virus, par exemple) à la sécurité des systèmes d'information ?

Par ailleurs, **il conviendrait de rendre obligatoire pour chaque ministère la tenue d'une cartographie à jour de son propre réseau informatique.** Cette cartographie devrait relever du fonctionnaire de la

sécurité des systèmes d'information, ce qui lui permettrait d'avoir une vision d'ensemble.

Enfin, dans l'attente de l'édification du Réseau Interministériel de l'Etat (RIE), il paraît indispensable de **contraindre les différents ministères à réduire le nombre de passerelles entre leurs réseaux et l'Internet et de développer les systèmes de surveillance de ces passerelles permettant de détecter les attaques.**

Compte tenu des risques soulevés par le *« cloud computing »* (ou « informatique en nuage ») au sein de l'administration, il semble également impératif de prévoir une obligation de localisation des données informatiques administratives sensibles ou celles appartenant au patrimoine informationnel de la Nation sur le territoire français. Certains acteurs pouvant être soumis à des législations autres que nationales, la solution s'appuyant sur un ***« cloud souverain »***, disposant d'infrastructures et services propres à l'Etat semble la seule à présenter les garanties nécessaires.

S'agissant plus particulièrement du **ministère de la défense et des armées**, l'organisation actuelle mériterait d'être confortée tout en prévoyant, à l'instar des autres ministères, un rehaussement du statut du fonctionnaire de la sécurité des systèmes d'information. Le fonctionnaire de la sécurité des systèmes d'information devrait voir sa place renforcée au sein de la direction générale des systèmes d'information et de communication (DGSIC) et en particulier disposer d'une réelle autorité sur la sous-direction et les équipes chargées de la sécurité des systèmes d'information au sein de la DGSIC.

Surtout, et en dépit des mesures déjà prises ou annoncées[1], votre rapporteur ne peut que déplorer **la faiblesse actuelle des effectifs et les moyens dédiés à la protection et à la défense des systèmes d'information au sein du ministère de la défense et des armées.**

Ainsi, comme cela a été mentionné précédemment, le CALID ne compte actuellement qu'une vingtaine de militaires, alors que la structure équivalente au Royaume-Uni en compte 80, soit quatre fois plus. Ses effectifs devraient passer à une trentaine en septembre 2012 et à quarante en 2013. Mais, dans le même temps, le champ d'action du CALID doit s'étendre aux systèmes tactiques des armées et à l'ensemble de l'informatique embarquée dans les systèmes d'armes et les plates-formes de combat.

La colocalisation du CALID avec le centre opérationnel de l'ANSSI (COSSI) au second semestre 2013 devrait certes permettre de renforcer les synergies et la coopération entre les deux entités.

Mais il paraît indispensable **d'augmenter sensiblement dans les prochaines années les ressources humaines et financières consacrées à la cyberdéfense au sein du ministère de la défense et des armées, comme d'ailleurs de la DGA et des services spécialisés.**

---

[1] *Voir le « plan de renforcement lutte informatique defensive/sécurité des systèmes d'information 2013-2016 » de 2011 et le « schéma directeur de la cybersécurité 2013-2018 » de juin 2012*

Au demeurant, cette augmentation régulière des effectifs, de l'ordre de quelques dizaines par an, ce qui représenterait 180 postes supplémentaires d'ici 2016 et 100 postes supplémentaires à l'horizon 2018, soit une progression de 280 postes pour la période 2012-2018 et cela pour l'ensemble du volet défensif, devrait rester modeste au regard du total des effectifs et du budget global du ministère de la défense, mais aussi au regard des enjeux.

Pourquoi ne pas utiliser aussi **les compétences de nos réservistes**, tant au sein de la réserve opérationnelle que de la réserve citoyenne, pour former une sorte de « cyber réserve » ?

Il semblerait également utile **d'encourager et de soutenir le rôle de la DGA en matière de conception et de certification de produits de haut niveau de sécurité pour les besoins militaires, ainsi que pour les produits civils ou interministériels.**

Enfin, d'une manière plus générale, même si notre pays dispose d'une législation assez complète et efficace, il paraît nécessaire d'introduire, dans le code de la défense, des **modifications législatives** visant à donner les moyens à l'ANSSI, aux armées et aux services spécialisés d'exercer leurs missions.

Cela concerne notamment **les domaines suivants** :

- l'autorisation de **la rétroconception**, c'est-à-dire la possibilité de « démonter », pour des motifs de sécurité, un logiciel ou un système ayant servi à une attaque informatique ;

- la possibilité de procéder à **l'analyse de comportement des codes malveillants**, de façon à suivre leur évolution, détecter leurs cibles d'attaque et anticiper leur mutation ;

- la possibilité de mettre en place des **dispositifs permettant de suivre les actions d'un attaquant ;**

- **l'identification et la collecte de vulnérabilités des outils utilisés par l'attaquant** ;

- **l'identification et les tests de vulnérabilités** concernant **les automates connectés à l'Internet**.

Enfin, pour reprendre l'une des préconisations du rapport Lasbordes, il semblerait utile d'instituer **un pôle juridictionnel spécialisé et centralisé pour réprimer les atteintes graves aux systèmes d'information**.

Les pôles spécialisés ont fait la preuve de leur efficacité, qu'il s'agisse de la lutte contre le terrorisme ou de la lutte contre le blanchiment. Compte tenu de la complexité des atteintes graves aux systèmes d'information, qui nécessitent souvent de passer par l'entraide internationale, il semblerait utile de disposer de magistrats spécialisés, spécialement formés à ces questions, regroupés au sein d'un pôle centralisé, ce qui permettrait également de renforcer la coopération entre les services spécialisés de la police et de la gendarmerie et la Justice.

3. Une doctrine publique sur les capacités « offensives » ?

En présentant le Livre blanc sur la défense et la sécurité nationale, le 17 juin 2008, l'ancien Président de la République M. Nicolas Sarkozy avait annoncé que face aux attaques informatiques, la France serait dotée « *de **capacités défensives et offensives**, qui concernent aussi bien toutes les administrations que les services spécialisés et les armées* ».

On peut parler de capacités offensives dès lors qu'il ne s'agit plus de protéger le système attaqué, mais d'identifier l'adversaire, de mettre à jour son mode opératoire, de le neutraliser, voire de lui appliquer des mesures de rétorsion.

Il convient de distinguer les missions qui relèvent des services de renseignement et la mise en place de capacités spécifiquement militaires.

S'agissant des **services de renseignement**, le Livre blanc de 2008 a prévu un développement des capacités techniques consacrées au réseau internet, « *devenu crucial pour notre sécurité* ». Le renforcement des moyens techniques devant s'accompagner d'une augmentation du nombre de techniciens et d'experts spécialisés dans ce domaine.

En ce qui concerne les forces armées, le Livre blanc de 2008 estimait nécessaire d'acquérir une **capacité de lutte informatique offensive** destinée notamment à neutraliser les centres d'opérations adverses.

Cette capacité suppose un **cadre** et une **doctrine d'emploi**, le développement d'outils spécialisés (armes numériques de réseaux, laboratoires technico-opérationnels), en préalable à la réalisation de véritables capacités opérationnelles, et la mise en œuvre d'une formation adaptée et régulièrement actualisée des personnels. Le Livre blanc précise que ce cadre d'emploi devra respecter le principe de riposte proportionnelle à l'attaque et viser en priorité les moyens opérationnels de l'adversaire.

En dépit d'incontestables difficultés liées par exemple à l'impossibilité d'établir avec certitude l'identité des agresseurs ou la responsabilité d'un Etat dans l'agression, votre rapporteur voit au moins **trois raisons qui militent en faveur du développement de capacités offensives** en matière informatique :

- la première, d'ordre technique, est que l'on se défend d'autant mieux que l'on connaît les méthodes et les moyens d'attaque et que de nombreux outils informatiques peuvent servir aux deux ;

- la deuxième, d'ordre plus stratégique, est qu'une telle capacité est très certainement de nature à jouer un rôle dissuasif vis-à-vis d'agresseurs potentiels ;

- enfin, le cyberespace paraît inévitablement voué à devenir un domaine de lutte, au même type que les autres milieux dans lesquels interviennent nos forces armées ; il est légitime d'en tirer les conséquences,

une telle capacité pouvant avoir des effets, tant aux niveaux tactique, opérationnel que stratégique.

Votre rapporteur est donc favorable à la poursuite du développement de « capacités offensives », sur la base d'un cadre juridique et d'une doctrine d'emploi bien définis.

Dans le même temps, il considère indispensable qu'**un contrôle parlementaire** s'exerce sur ces activités, qui, compte tenu de leur caractère très sensible, ne peut relever que de **la délégation parlementaire au renseignement.**

Une autre interrogation, qui n'est pas sans importance, porte sur le fait de savoir s'il est possible et souhaitable pour un Etat de définir **une doctrine publique**, ou du moins de tenir **un discours public**, sur les « capacités offensives ».

Comme on l'a vu précédemment avec le cas de STUXNET, si les autorités américaines n'ont jamais reconnu jusqu'à présent avoir utilisé des armes informatiques, elles reconnaissent en revanche développer de telles capacités et elles n'hésitent pas affirmer publiquement qu'elles pourraient en faire usage, notamment pour répondre à une attaque informatique massive.

Une telle doctrine publique sur les « opérations dans le cyberespace » se retrouve ainsi dans le rapport du département de la défense au Congrès de novembre 2011 consacré au cyberespace[1]. D'après ce document, *« le Président des Etats-Unis se réserve le droit de répondre par tous moyens, y compris par des capacités cybernétiques, à un acte hostile dans le cyberespace dirigée contre les Etats-Unis, ses alliés ou partenaires ou ses intérêts, telle qu'une attaque informatique »*. Et, il est indiqué plus loin que *« le département de la défense a les capacités de conduire des opérations (offensives) dans le cyberespace pour défendre la Nation, ses alliés et ses intérêts »*.

Comme l'a indiqué à votre rapporteur, M. James Lewis, expert du *Center for Strategic and International Studies* (CSIS), lors de sa visite à Washington, à la suite des révélations sur l'affaire STUXNET, l'administration présidentielle américaine travaillerait actuellement à préciser certains points importants.

Il s'agirait de répondre aux questions suivantes : Qui peut autoriser une cyberattaque ? Dans quel cas le Président doit agir ? Quels devraient être les rôles respectifs du Président et des militaires ? Le centre de commandement doit-il intervenir de manière indépendante ou bien être intégré au sein du centre de planification et de conduite des opérations ?

Selon un rapport du CSIS de décembre 2011, au moins trente-cinq Etats auraient développé une doctrine militaire en matière de « cyberguerre ».

---

[1] *Department of Defense Cyberspace Policy Report, " A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011, Section 934, november 2011*

Ainsi, d'après le Département de la défense américain, la Chine a intégré depuis longtemps la lutte informatique comme une partie intégrante de sa stratégie militaire. Elle y voit le moyen de compenser, par des moyens peu coûteux, l'infériorité de ses moyens conventionnels. Elle dispose à cet effet d'un immense réservoir humain, et n'est donc pas entravée par les limites physiques tenant au nombre d'opérateurs qui pourraient rendre moins efficaces des attaques de grande ampleur.

Bien que l'on ne dispose bien évidemment d'aucune source officielle à ce sujet, la Chine aurait concentré au sein de l'**Armée populaire de libération** la totalité de ses capacités étatiques, tant défensives qu'offensives. Toujours selon les militaires américains, les planifications d'un éventuel conflit avec Taïwan intégreraient le ciblage des systèmes d'information, notamment ceux utilisés pour les flux logistiques, moins protégés que les systèmes opérationnels. Si l'armée chinoise semble disposer d'un département spécialisé doté de moyens conséquents, on ne peut exclure que le gouvernement chinois s'appuie également sur les nombreux groupes de pirates informatiques.

D'autres pays, à l'image du Japon, de l'Inde ou d'Israël[1] par exemple, reconnaissent **publiquement** développer des capacités offensives, même s'ils déclarent généralement limiter l'usage de ces capacités à une riposte en cas d'attaque, ce que l'on peut toutefois qualifier de palinodie.

Certes, il ne faut pas négliger les inconvénients pour notre pays qu'il y aurait à évoquer publiquement ce sujet, qui tiennent essentiellement à la crainte de donner une sorte de légitimité aux attaques informatiques d'origine étatique et d'encourager ainsi les autres pays à développer et à utiliser de telles capacités, ainsi que le risque de dévoiler aux yeux de tous l'étendue de notre expertise dans ce domaine, ce qui pourrait conduire à affaiblir la portée de ces capacités.

Il ne paraît pas évident en effet pour un Etat de reconnaître publiquement vouloir se doter d'armes informatiques, étant donné que toute intrusion dans un système informatique est généralement condamnée par la loi, surtout lorsque ces mêmes pays n'hésitent pas à dénoncer publiquement les attaques informatiques dont ils sont victimes, en particulier lorsqu'elles proviennent d'autres Etats.

Toutefois, le silence absolu des autorités françaises sur cette question depuis le Livre blanc de 2008 paraît quelque peu en décalage avec l'évolution de la menace, les communications publiques de nos principaux partenaires, et il pourrait même être de nature à entretenir des fantasmes dans l'opinion publique.

---

[1] *Le ministère israélien de la défense a ainsi rendu public sur le site Internet de l'armée une doctrine sur la « cyberguerre » précisant les méthodes et les objectifs des opérations militaires dans le cyberespace, considéré comme un nouveau « champ de bataille », à côté des autres milieux de la terre, de la mer, de l'air et de l'espace*

Surtout, le développement de « capacités offensives » nécessite une anticipation opérationnelle, une préparation technique et un travail très important, portant non seulement sur l'arme informatique elle-même, mais aussi sur le recueil de renseignement, la désignation de cibles potentielles, l'analyse des systèmes d'information ainsi que leur environnement, l'identification des vulnérabilités, avec la nécessité de procéder à des entraînements en liaison étroite avec d'autres modes d'interventions (armes conventionnelles, missiles balistiques, etc.) ou encore un travail sur la définition même d'une « arme informatique » et les conditions de son emploi dans le cadre du droit des conflits armés.

Dès lors, votre rapporteur est plutôt enclin à penser qu'**il serait souhaitable que les autorités françaises lancent une réflexion sur l'élaboration d'une éventuelle doctrine ou du moins d'un discours ayant vocation à être rendu publics sur les « capacités offensives ».**

Une telle doctrine ou un tel discours présenteraient le mérite, en particulier s'ils étaient portés au plus haut niveau de l'Etat, de donner un fondement incontestable à ces capacités et, dans le même temps, de préciser à l'opinion publique certaines règles d'emploi. Il ne faut pas négliger non plus l'effet dissuasif qu'ils pourraient avoir sur de potentiels adversaires.

Pour ces raisons, votre rapporteur souhaite que dans le contexte de l'élaboration du futur Livre blanc **une réflexion s'engage sur l'intérêt et le contenu d'une telle doctrine**, afin que, si cette idée recueille un large assentiment, cette doctrine soit reprise dans le contenu du nouveau Livre blanc.

Peut-on pour autant dresser un parallèle avec la dissuasion nucléaire et considérer que le développement de capacités offensives participe à une sorte de « dissuasion dans le cyberespace » ?

Votre rapporteur ne le pense pas. En effet, l'arme informatique présente au moins trois différences avec l'arme nucléaire :

- à la différence d'une attaque nucléaire, il est très difficile, voire impossible, d'identifier précisément et de façon certaine l'auteur d'une attaque informatique qui cherche à rester discret ;

- la dissuasion nucléaire repose sur une relation d'Etat à Etat, qui est inopérante face à une menace asymétrique comme les attaques informatiques, qui sont le plus souvent l'œuvre de *« pirates informatiques »* ou d'organisations, même si ces attaques peuvent aussi parfois être instrumentalisées ou même être dirigées par des Etats ;

- enfin et surtout, l'arme nucléaire est une arme de non emploi, alors que les attaques informatiques sont une réalité concrète et quotidienne.

Aux yeux de votre rapporteur, il est donc préférable, afin d'éviter toute confusion, de ne pas employer le terme de *« cyberdissuasion »* et d'éviter la comparaison avec la dissuasion nucléaire.

B. RENFORCER LE PARTENARIAT AVEC L'ENSEMBLE DES ACTEURS

La **coopération avec le secteur privé** est encore insuffisamment développée en France alors qu'elle constitue **une dimension essentielle**, comme en témoigne la place éminente accordée à ce volet dans les stratégies cyber mises en place aux Etats-Unis, au Royaume-Uni ou en Allemagne.

Pour votre rapporteur, il importe d'accentuer nos efforts dans trois directions : le développement du **partenariat avec le secteur économique**, le renforcement des relations avec **les opérateurs d'importance vitale**, et, enfin, en matière de formation, de recherche, de sensibilisation et de communication.

1. Développer le partenariat avec le secteur économique

La sensibilisation des entreprises, et singulièrement de leurs dirigeants, aux enjeux liés à la sécurité des systèmes d'information mériterait tout d'abord d'être fortement renforcée.

Assurer la sécurité des systèmes d'information des entreprises n'est pas seulement un enjeu technique. C'est aussi un double enjeu économique et stratégique, puisqu'il s'agit de protéger l'ensemble des maillons de la chaîne de valeur des entreprises, notre savoir-faire technologique comme nos parts de marché, dans la véritable guerre économique que nous connaissons aujourd'hui, voire un enjeu politique, lorsque les intérêts de la Nation sont en jeu.

Or, avec l'espionnage informatique, notre pays, comme d'autres pays, est aujourd'hui menacé par un « pillage » systématique de son patrimoine diplomatique, culturel, scientifique et économique. Ainsi, les efforts consentis par les entreprises françaises pour augmenter leur compétitivité via des investissements importants en matière de système d'information se révèlent, en cas d'espionnage, servir leurs concurrents. C'est l'un des aspects masqués d'une mondialisation déloyale qu'il faut rendre plus visible.

Et ce danger ne peut que s'accentuer avec le développement dans les entreprises de pratiques comme le *« BYOD » (« Bring Your Own Device »)*, le *« cloud computing »* (« informatique en nuage »)[1] ou encore l'utilisation des réseaux sociaux, qui présentent des risques majeurs du point de vue de la sécurité des systèmes d'information.

La protection des systèmes d'information devrait être **une véritable priorité en matière de management des entreprises**. Les dirigeants des entreprises, les membres du conseil d'administration devraient être davantage sensibilisés. Cet aspect mériterait d'être pris en compte dans le bilan annuel, le rapport de gestion et dans les discussions au sein du conseil d'administration[2].

---

[1] *Voir le glossaire qui figure en annexe*

[2] *On peut à cet égard mentionner l'obligation pour les entreprises américaines de publier les incidents et les risques majeurs dans les bilans boursiers trimestriels*

Le niveau hiérarchique, les responsabilités et le rôle des responsables de la sécurité informatique devraient également être rehaussés au sein des entreprises.

Faut-il aller plus loin et recourir à la loi pour poser un certain nombre de règles ou de principes ?

Faut-il ainsi prévoir **une déclaration obligatoire ou systématique** à l'ANSSI en cas d'attaque importante contre les systèmes d'information des entreprises, en s'inspirant des mesures mises en place ou à l'étude chez certains de nos partenaires ? Est-il réellement utile de rendre publiques ces attaques, à l'image de ce qui existe aux Etats-Unis ? Cette obligation doit-elle être assortie de sanctions et de quelle nature ? Et, comment mettre en place une procédure permettant de contrôler le respect de cette prescription ? Ne serait-il pas plus opportun d'inciter les entreprises à faire une telle déclaration au moyen de mesures incitatives ?

Votre rapporteur, réservé à l'égard de l'« inflation législative » et soucieux de ne pas alourdir les charges administratives qui pèsent sur les entreprises, a beaucoup hésité sur cette question.

En définitive, après avoir beaucoup consulté, votre rapporteur a acquis la conviction qu'une telle obligation de notification serait de nature à renforcer la sensibilisation des entreprises à la menace et qu'elle permettrait à l'Etat d'être réellement informé de ces attaques.

Naturellement, une telle déclaration ne peut se concevoir que dans le cadre d'une stricte confidentialité de la part des services de l'Etat, compte-tenu des craintes légitimes des entreprises pour leur image, mais aussi des conséquences économiques potentielles d'une éventuelle révélation publique.

Votre rapporteur est donc convaincu de l'intérêt de prévoir **une déclaration obligatoire (et confidentielle) des entreprises en cas d'attaque importante sur leurs systèmes d'information.**

Dans le même temps, votre rapporteur considère qu'une telle obligation ne devrait pas nécessairement s'accompagner de sanctions mais plutôt de **mesures incitatives afin d'inciter les entreprises à renforcer la protection de leurs systèmes d'information.**

Dans certains pays, comme les Etats-Unis, des modifications ont été introduites dans la législation pour inciter les entreprises à renforcer la protection de leurs systèmes d'information, au moyen d'**une limitation de responsabilité** pour les entreprises dont le respect des bonnes pratiques est confirmé par des audits réguliers ou encore d'**une préférence dans le cadre des marchés publics** pour les entreprises qui souscrivent aux recommandations de l'administration concernant la protection de leurs systèmes d'information.

Pour votre rapporteur, il semblerait utile d'engager en France une réflexion avec **les compagnies d'assurance** sur la prise en charge des

opérations de traitement d'une cyberattaque. La compagnie d'assurance pourrait s'engager à compenser en tout ou partie les pertes financières résultant du traitement d'une attaque informatique à condition que l'entreprise concernée ait mis en place des mesures dans ce domaine (moyennant un certain niveau de sécurité initial, l'utilisation d'équipements labellisés, l'existence d'une politique en matière de sécurité des systèmes d'information ou encore un audit annuel par exemple).

Pourquoi ne pas imaginer aussi **un système de notation**, à l'image de ce qui existe en matière financière ou de respect de l'environnement ? L'inconvénient d'un tel système résiderait toutefois dans le fait qu'il pourrait donner lieu à une sorte d'« appel au défi » lancé aux pirates informatiques désireux de prouver qu'ils sont en mesure de contourner les mesures de protection jugées les plus robustes.

D'une manière plus générale, les entreprises les plus concernées par la sécurité des systèmes d'information (opérateurs d'importance vitale, entreprises intervenant dans des domaines sensibles) attendent, votre rapporteur l'a constaté lors de ses auditions, **des échanges d'informations beaucoup plus fournis et des contacts beaucoup plus fréquents avec les services de l'Etat**.

L'ANSSI devrait ainsi être en mesure de répondre aux demandes des entreprises, en matière **d'expertise, de conseils, d'assistance et d'offre de produits labellisés**.

Le partenariat avec le secteur privé doit également contribuer au **soutien à la base industrielle et technologique** en matière de produits et de services de sécurité des systèmes d'information, notamment à l'égard des PME-PMI du secteur, et plus largement, dans le secteur des technologies de l'information et de la communication.

De même qu'il existe en France une base industrielle et technologique de défense (BITD), votre rapporteur considère qu'il devrait exister **une base industrielle et technologique en matière cyber** (BITC).

La France dispose d'atouts importants avec des grandes entreprises, à l'image de Cassidian, la division défense et sécurité du groupe EADS, de THALES, de BULL, de SOGETI ou d'ALCATEL-LUCENT, spécialisées et renommées pour leur expertise dans le domaine de la sécurité des systèmes d'information.

On trouve également en France un tissu de PME-PMI innovantes, à l'image de Netasq et d'Arkoon en matière de logiciels et produits de sécurité ou de Sysdream, d'Atheos et de DevoTeam en matière de services.

Notre pays dispose ainsi de véritables « trésors nationaux » dans certains domaines clés pour la défense et la sécurité des systèmes d'information, comme la cryptologie ou les cartes à puces.

Si le marché mondial est aujourd'hui dominé par des sociétés américaines et israéliennes, et, demain, par des sociétés chinoises, russes et indiennes, la France pourrait, si elle en a la volonté, développer une industrie complète et souveraine dans le domaine de la sécurité des systèmes d'information, à la fois dans les secteurs des matériels, des logiciels et des services.

Aux yeux de votre rapporteur, **il est crucial pour notre pays de conserver une autonomie stratégique** dans un domaine qui joue un rôle de plus en plus important dans les domaines de la défense et de la sécurité. Afin de garantir la souveraineté des opérations stratégiques ou vitales, il est indispensable de s'assurer de la maîtrise de certaines technologies fondamentales, dans des domaines comme la cryptologie, l'architecture matérielle ou logicielle des équipements de sécurité ou encore les systèmes d'exploitation. On ne doit pas négliger non plus les enjeux économiques et en matière d'emplois dans un secteur en forte croissance et qui participe à la compétitivité d'un pays.

Toutefois, le secteur des fournisseurs français de solutions en sécurité des systèmes d'information souffre aujourd'hui de **plusieurs lacunes** :

- une **trop grande fragmentation**, qui entraîne souvent une concurrence destructrice entre les entreprises françaises et entrave le développement des PME et l'émergence d'entreprises de taille intermédiaire ;

- **une difficulté d'accès à la commande publique** pour les PME-PMI ;

- un problème majeur **d'accès au financement** pour les PME, qui ne peuvent recourir à l'emprunt bancaire ;

- **un positionnement trop « franco-français »** pour assurer le développement de groupes solides, exporter et gagner des parts de marché à l'étranger ou nouer des partenariats à l'échelle européenne ou mondiale.

L**'Etat devrait donc soutenir, par une politique industrielle volontariste, le tissu industriel des entreprises françaises, notamment des PME, proposant des produits ou des services importants pour la sécurité informatique.**

L'Etat devrait ainsi encourager **une consolidation structurelle et capitalistique du secteur**, en impliquant les PME avec des positionnements complémentaires et une volonté partagée, les financeurs publics (comme la caisse des dépôts et consignations ou encore la banque publique des PME) et privés (fonds d'investissements), ainsi que la puissance publique. L'objectif serait de favoriser l'émergence de « champions nationaux » ou européens.

Il paraît également souhaitable de privilégier, dans le cadre de la commande publique, les solutions et sociétés françaises, via les certifications et évaluations de sécurité réalisées par l'ANSSI.

Ne pourrait-on pas envisager également que **les PME se regroupent ou s'associent, éventuellement autour de grands groupes, pour mutualiser leurs solutions en produits sécurisés** ?

L'allégement de la procédure de certification, la réduction des coûts et le raccourcissement des délais constituent également de fortes attentes des entreprises du secteur.

Les entreprises attendent aussi de l'Etat **un renforcement du soutien à la promotion et à l'export** concernant les produits de sécurité informatique.

L'Etat devrait encourager le regroupement des entreprises à l'export, notamment entre les grandes entreprises et les PME, dans le cadre d'une *« chasse en meute »* ou d'un partenariat plus intégré, et leur apporter un soutien, par exemple en leur fournissant des informations sur les marchés d'export, les entreprises étrangères concurrentes ou les partenaires potentiels, en les accompagnant dans leurs démarches et dans la promotion de leurs offres à l'étranger, etc.

De même qu'il existe des « salons de l'armement », à l'image du salon du Bourget ou d'Eurosatory, pourquoi ne pas imaginer de créer en France **un salon spécialisé** sur la cybersécurité, afin de donner plus de visibilité aux entreprises françaises de ce secteur ?

Le **financement public de la recherche-développement** en matière de sécurité des systèmes d'information doit aussi être accentué et cette recherche partagée entre les différents acteurs publics.

Le fonds interministériel de soutien à l'innovation que le plan de renforcement de la sécurité des systèmes d'information avait préconisé n'a pas été mis en place et les différentes sources de financement restent dispersées.

Il existe certes des instruments importants comme le crédit-impôt recherche, le dispositif d'avance remboursable d'OSEO ou encore le label « jeune entreprise innovante ». Mais les entreprises, et en particulier les PME qui souhaitent développer leur activité, rencontrent encore de fortes difficultés en matière d'accès au financement.

Ainsi, dans le cadre du crédit-impôt recherche, la tendance en France est de considérer que seules les dépenses liées à la recherche et développement sont éligibles, alors que les dépenses de marketing et de développement commercial, notamment à l'international, sont souvent négligées, alors même qu'elles déterminent en grande partie la réussite du projet. Le financement de l'amorçage, à l'image du *« Business Angels »* aux Etats-Unis, n'existe quasiment pas en France, et le capital-risque est quasiment inexistant dans ce secteur.

Ce **dispositif doit donc être clarifié**, en vue notamment d'en faciliter l'accès par les PME-PMI innovantes dans le domaine de la sécurité des systèmes d'information.

Afin de clarifier ce dispositif on pourrait imaginer la création d'**un fonds public spécialisé dans la sécurité et la confiance numérique**, dans le cadre du Fonds national pour la société numérique (FSN), et qui serait notamment chargé de l'amorçage et du capital risque.

D'une manière générale, les échanges d'information entre l'ANSSI et les entreprises françaises du secteur de la sécurité des systèmes d'information mériteraient d'être sensiblement renforcés.

En s'inspirant du programme lancé par le département de la défense aux Etats-Unis, on pourrait mettre en place entre l'ANSSI et les entreprises du secteur de la sécurité des systèmes d'information, une sorte de « club », un **réseau des prestataires de confiance**, afin de développer les échanges entre le secteur public et le secteur privé.

Un tel réseau pourrait notamment jouer un rôle utile en matière de ressources humaines, pour encourager la formation et la mobilité des ingénieurs spécialisés dans la protection des systèmes d'information, ou encore pour échanger des informations sur les vulnérabilités de certains produits et les moyens de s'en protéger. Il pourrait également être activé en cas de détection de cyberattaque ciblée, pour aider les entreprises à mettre en place les contre-mesures nécessaires.

2. Assurer la protection des systèmes d'information des opérateurs d'importance vitale

Dans un rapport remis au Secrétaire général de la défense et de la sécurité nationale, portant sur *« les réponses aux nouvelles cybermenaces sur les systèmes d'information, de communication et de production d'importance vitale »*, d'avril 2011, le Conseil général de l'industrie, de l'énergie et des technologies (CGIET), rebaptisé depuis Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET), organisme rattaché au ministère de l'économie et des finances, a formulé une série de recommandations afin de renforcer la protection des opérateurs d'importance vitale, préconisations qui n'ont pas été rendues publiques.

Votre rapporteur, qui s'est longuement entretenu avec les auteurs de ce rapport, estime que **la sécurité des systèmes d'information des opérateurs d'importance vitale constitue aujourd'hui la principale lacune du dispositif français et qu'il est indispensable qu'elle soit érigée en véritable priorité nationale.**

Il importe d'abord de renforcer les échanges entre l'ANSSI et les opérateurs d'importance vitale, sur une base sectorielle.

Les opérateurs d'importance vitale attendent, en effet, de l'Etat des informations sur l'état de la menace, les vulnérabilités et les moyens de protection, alors que l'ANSSI a besoin de connaître l'état de la situation.

Pour votre rapporteur, il conviendrait de **rendre obligatoire** pour tous les opérateurs d'importance vitale :

- **une déclaration d'incident à l'ANSSI** dès la détection d'un incident informatique susceptible de relever d'une attaque contre les systèmes d'information ;

- le maintien d'une **cartographie à jour** des systèmes d'information ;

- une **déclaration à l'ANSSI de systèmes de contrôle des processus ou des automates industriels** (SCADA) connectés à l'Internet ;

- un **audit annuel en matière de sécurité des systèmes d'information**, dont les résultats devraient être tenus à la disposition de l'autorité nationale de défense des systèmes d'information ;

- la **réduction du nombre de passerelles entre les réseaux et l'Internet** et le déploiement de **systèmes de surveillance des flux** permettant de détecter les attaques informatiques, agréé par l'ANSSI et favoriser le groupement d'opérateurs d'importance vitale autour de **systèmes de détection partagés**, opérationnels 24 heures sur 24, 7 jours sur 7.

3. Encourager la formation, soutenir la recherche et accentuer la sensibilisation

Il existe en France peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les administrations ainsi que les entreprises rencontrent des difficultés pour en recruter.

D'après les informations recueillies par votre rapporteur, il y aurait dans ce domaine **quatre à cinq fois plus** d'offres d'emplois disponibles, dans les administrations ou les entreprises, que d'ingénieurs spécialement formés à la sécurité informatique sortant des écoles d'ingénieurs.

Il apparaît donc indispensable d'encourager les écoles d'ingénieurs à **développer des formations en matière de sécurité des systèmes d'information.**

Plus généralement, la protection des systèmes d'information devrait être une étape obligée dans le cursus de l'ensemble des formations d'ingénieurs ou d'informatique, avec un module spécifique.

Trop d'ingénieurs ou d'informaticiens sortent, en effet, des écoles d'ingénieurs ou d'informatique sans avoir été jamais sensibilisés à l'importance d'assurer la protection des systèmes d'information.

De manière plus générale, il semblerait utile d'inclure **une sensibilisation obligatoire dans les écoles formant les cadres de l'administration (comme l'ENA par exemple) et de proposer une telle sensibilisation aux formations de management destinées aux entreprises**.

Une autre priorité concerne **le soutien à la recherche.**

Si la France dispose de centres d'excellence reconnus dans certains domaines clés pour la défense et la sécurité des systèmes d'information, comme celui de la cryptologie ou des cartes à puces, de manière générale, **la recherche semble insuffisamment développée en France.**

Cela concerne en premier lieu les filières scientifiques, comme l'informatique, mais aussi d'autres disciplines, comme les sciences humaines ou sociales, le droit, la géostratégie, etc.

Notre pays manque ainsi cruellement de laboratoires travaillant sur des sujets clés, essentiels à une réelle maîtrise des enjeux nationaux en termes de sécurité des systèmes d'information.

En dehors de certaines initiatives récentes, telles que la création par l'Institut des hautes études de la défense et de la sécurité nationale (IHEDN), avec le soutien de EADS Cassidian, d'une chaire Castex de cyberstratégie dirigée par le professeur M. François Géré, l'organisation d'un séminaire consacré à la sécurité numérique par l'Institut national des hautes études de la sécurité et de la justice (INHESJ) animé par M. Nicolas Arpagian ou encore l'inauguration, le 2 juillet dernier, de la chaire cyberdéfense des écoles de Saint-Cyr Coëtquidan, en partenariat avec Sogeti et Thales, ce sujet ne semble pas susciter l'attention qu'il mérite de la part des universités, des grandes écoles ou des centres de recherche. Ainsi, on dénombre peu de chercheurs ou de spécialistes de ces questions, même s'il existe quelques experts reconnus, comme MM. Nicolas Arpagian, Olivier Kempf et Daniel Ventre, avec lesquels votre rapporteur s'est d'ailleurs entretenu.

Par ailleurs, notre pays souffre d'un **manque de stratégie commune** et de **l'éparpillement des différents organismes publics de recherche** (CNRS, INRIA, CEA-LETI)**,** qui s'ignorent le plus souvent et d'une coopération insuffisante de ces organismes avec l'ANSSI ou la DGA.

Afin de renforcer la cohérence et l'efficacité de notre dispositif, il semblerait utile que l'Etat fixe des objectifs en matière de recherche et développement en matière de cybersécurité à l'ANSSI, à la direction générale de l'armement ainsi qu'aux autres organismes de l'Etat.

On pourrait également envisager la création d'un **budget spécifique de recherche et développement dans ce secteur**, de type *« budget civil de recherche et développement »* (BCRD), qui regroupe l'ensemble des crédits publics consacrés à la recherche civile et au développement technologique, à l'image de ce qui a été fait pour soutenir le Centre national d'études spatiales (CNES).

De même qu'il existe un comité mixte sur l'armement nucléaire, regroupant le Commissariat de l'énergie atomique et les armées, il pourrait être utile de rapprocher l'ANSSI, la DGA, l'INRIA, le CEA-LETI et les laboratoires concernés du CNRS, en créant un comité mixte sur la recherche en matière de protection et de défense des systèmes d'information, ou du moins un comité stratégique visant à coordonner les efforts.

Afin de renforcer la recherche et de rapprocher les différents acteurs publics, mais aussi l'Etat, les entreprises, les universités et les centres de recherches, la création d'**une fondation** serait actuellement à l'étude.

Cette fondation doit se former sur la base d'un partenariat entre le secteur public et le secteur privé avec un financement mixte provenant de fonds publics et privés. Elle devrait avoir comme premier objectif d'identifier les laboratoires ayant une réelle expertise dans les domaines qui semblent aujourd'hui insuffisamment pilotés et partagés. Cette fondation pourrait également encourager la recherche dans des domaines délaissés jusqu'à présent au niveau national, notamment par le financement de chaires, de bourses de thèses et de post-doctorat, de centres de recherches, de laboratoires, et par la valorisation de cette recherche au travers de séminaires, de formations ou de stages, et de la publication des résultats de ces travaux, le tout dans une optique pluridisciplinaire.

Pour votre rapporteur, **la création d'une telle fondation** apparaît, en effet, **souhaitable**, car elle participe à la construction d'une vision prospective, au niveau national, à une meilleure évaluation des risques et des menaces et au renforcement des mesures permettant d'y faire face. Elle contribuera aussi à renforcer la présence et l'influence de la France au niveau international dans un domaine largement dominé actuellement par des laboratoires situés outre-Atlantique.

Il semble également souhaitable **d'encourager et de développer le rôle des sociétés privées de conseil et d'assistance en matière de sécurité informatique**.

Comme cela a été confirmé à votre rapporteur lors de ses auditions, l'activité des sociétés privées de conseil et d'assistance en matière de sécurité informatique n'est pas encore suffisamment reconnue en France et se heurte toujours à des difficultés juridiques.

La France dispose pourtant de sociétés de conseil en sécurité informatique aux compétences reconnues, à l'image de Sysdream, qui réalise notamment des formations et des audits pour le ministère de la défense et pour de grandes entreprises et dont votre rapporteur a rencontré des représentants.

Comment expliquer, par exemple, que la législation française interdit la communication, même à des fins de conseils aux entreprises ou de recherche, de failles dans les systèmes d'information décelées lors d'une intrusion informatique ?

C'est pourtant le meilleur moyen de sensibiliser une entreprise à assurer une plus grande protection de ses systèmes d'information.

D'ailleurs, certaines entreprises américaines, à l'image de Microsoft ou de Facebook, ne s'y sont pas trompées, en lançant un appel public à tous les « hackers » pour déceler les vulnérabilités de leurs systèmes informatiques, réalisant ainsi gratuitement et à l'échelle mondiale un audit de leur sécurité informatique.

Il semble donc souhaitable de reconnaître, par un système d'agrément ou de label, et d'encourager l'activité de ces sociétés privées de conseil et d'assistance en matière de sécurité informatique, en soutenant leur activité, notamment auprès des entreprises, et en adaptant notre législation.

Plus largement, il conviendrait de **renforcer les liens** avec la *« communauté de hackers »* présente en France.

D'après les informations recueillies par votre rapporteur, la *« communauté des hackers »* serait estimée en France à environ 4 000 personnes. Nombre d'entre eux seraient désireux de mettre leurs compétences et leurs talents au service de notre pays.

Ainsi, selon M. Eric Filiol, directeur du laboratoire de sécurité informatique de l'Ecole supérieure internationale d'administration des entreprises (ESIAE), *« il faut chercher les ressources là où elles sont. Chez les hackers que l'on a tendance à diaboliser à l'excès »*[1].

Aux Etats-Unis, les *« communautés de hackers »* sont d'ailleurs largement reconnues et entretiennent des relations étroites avec les autorités chargées de la sécurité des systèmes d'information. On peut ainsi mentionner la communauté de *« hackers »* *« Defcon »*, qui compte plus de 12 000 membres aux Etats-Unis et qui entretient des relations avec le département de la défense et l'agence de sécurité nationale (NSA).

La plupart de ces *« hackers »* ne sont pas, en effet, des *« cybercriminels »* ou *« chapeaux noirs »*, mais des personnes capables d'analyser en profondeur un système informatique afin d'y déceler d'éventuelles vulnérabilités.

Leur objectif est de déceler des failles ou vulnérabilités dans les systèmes d'information, non pas dans une intention malveillante, mais au contraire dans un souci de corriger ces failles et renforcer ainsi la sécurité.

La principale motivation de ces *« chapeaux blancs »* ou *« chapeaux gris »* est, en effet, la renommée qu'ils peuvent acquérir au sein de leur communauté et auprès du public en publiant le résultat de leurs investigations.

Or, actuellement, notre législation ne permet pas la publication, même à des fins scientifiques, de vulnérabilités décelées à la suite d'intrusions dans les systèmes informatiques, ce qui oblige les « pirates informatiques » français à publier le résultat de leurs recherches dans les revues d'autres pays, notamment aux Etats-Unis, ou lors de conférences de *« hackers »*.

Comme le souligne M. Eric Filiol, *« depuis quatre ans, les avancées majeures en matière de cryptanalyse ne sont plus publiées dans les conférences académiques mais dans les conférences de hackers »*. À ses yeux, il existe une véritable fracture en France entre *« un monde d'anciens qui*

---

[1] *Valery Marchive, « Cyberguerre : l'impréparation reste la norme », lemagit, 20 septembre 2011*

administrent mais qui ne comprennent rien à la technique et de jeunes hackers qui maîtrisent mais qui n'administrent pas ».

Enfin, **la sensibilisation des usagers et du grand public mériterait d'être renforcée**, car, en définitive, la sécurité des systèmes d'information repose pour une large part sur un ensemble de règles de comportements qui relèvent des utilisateurs.

Or, ces règles, que le directeur général de l'ANSSI, M. Patrick Pailloux, qualifie souvent de « règles d'hygiène » élémentaires, sont le plus souvent largement ignorées par la plupart des utilisateurs qui les considèrent comme autant de contraintes.

Ainsi, des règles élémentaires, comme le choix de mots de passe robustes, la non utilisation d'équipements informatiques personnels, comme des ordinateurs portables, des clés USB, des ordiphones ou des tablettes, dans un cadre professionnel, la prudence à l'égard des liens et des pièces jointes contenus dans les courriels, ne sont pas respectées alors qu'elles représentent des conditions essentielles pour la sécurité des systèmes d'information.

Il importe donc **de renforcer les mesures de sensibilisation à destination des acteurs, comme du grand public**.

L'ANSSI a certes développé une politique de communication, avec, par un exemple un portail Internet consacré à la sécurité informatique[1], un petit guide de sécurité informatique destiné aux collaborateurs des cabinets ministériels ou encore un guide sur la sécurité informatique des systèmes industriels.

On peut également mentionner la création d'un logo spécifique[2], qui vise à renforcer la visibilité de l'ANSSI à l'extérieur :

[1] *http://www.securite-informatique.gouv.fr/*

[2] *A titre anecdotique, le logo de l'ANSSI contient un code caché sous forme de chiffres et de lettres que les spécialistes peuvent s'amuser à déchiffrer*

Mais, ces mesures restent très insuffisantes.

Si la compétence et l'efficacité de l'Agence nationale de sécurité des systèmes d'information sont unanimement reconnues, en France comme à l'étranger, comme votre rapporteur a pu lui-même le constater lors de ses différents déplacements, en revanche, sa notoriété est notoirement insuffisante et sa politique de communication est largement inaudible.

Ainsi, **n'est-il pas paradoxal que le portail de la sécurité informatique ou le site Internet de l'agence française de sécurité des systèmes d'information soient aussi ternes et peu attractifs pour les internautes**, avec notamment l'absence de tout moteur de recherche et des mises à jour aléatoires ?

Les informaticiens de l'agence sont pourtant réputés être les meilleurs de leur spécialité. Il devrait être relativement simple de rendre le site Internet de l'ANSSI et le portail plus attractifs et plus dynamiques, à l'image de ce qui existe d'ailleurs chez la plupart de nos partenaires étrangers.

De même, on peut regretter **l'absence de toute politique de communication de l'agence dirigée spécialement vers les PME**, alors même qu'elles sont les plus vulnérables aux attaques informatiques.

L'Agence pourrait, en liaison avec le ministère délégué chargé des PME, de l'innovation et de l'économie numérique, travailler avec les chambres de commerce et d'industrie, relais traditionnels vers les PME.

L'Agence devrait donc améliorer sa politique de communication – qu'il s'agisse des responsables politiques, des administrations, des entreprises ou du grand public. Ainsi, pourquoi ne pas diffuser plus largement la synthèse d'actualité de l'ANSSI sur les incidents informatiques, qui est actuellement envoyée à un nombre très restreint de personnes ?

Les **mesures de sensibilisation des utilisateurs** mériteraient également d'être fortement accentuées.

Cela passe notamment par l'établissement de chartes à l'usage des utilisateurs au sein des entreprises comme des administrations, par un développement de la communication et de la formation, etc.

Ainsi, il semblerait utile de développer le programme de formation de l'ANSSI et de l'élargir à d'autres publics, notamment issu du secteur privé.

La politique de sensibilisation à destination du **grand public** ne doit pas non plus être négligée.

De même qu'il existe un plan national de prévention en matière de sécurité routière, pourquoi ne pas imaginer également **un plan de communication en matière de sécurité des systèmes d'information** ?

Un exemple de mesure de sensibilisation :

Les 10 commandements de la sécurité sur l'internet

- Tu passeras tes supports amovibles sur une station blanche et tu ne connecteras pas de supports personnels sur une station professionnelle

- Tu effaceras toutes les données sensibles inutiles de tes clés USB avant de voyager

- Tu rendras compte de toute détection virale aux organismes compétents

- Tu vérifieras régulièrement qu'aucun équipement anormal n'est connecté sur ta station professionnelle

- Tu utiliseras des mots de passe robustes

- Tu ne laisseras pas ton mot de passe accessible

- Tu ne communiqueras ton adresse mail professionnelle qu'à des personnes de confiance

- Tu vérifieras l'expéditeur des mails que tu reçois

- Tu seras vigilant avant d'ouvrir des pièces jointes à un courriel

- Tu n'enverras pas de fichier sensible par Internet sans protection

Enfin, il semblerait souhaitable, aux yeux de votre rapporteur, que **les responsables politiques** de notre pays, y compris au plus haut niveau de l'Etat, **se saisissent des enjeux liés à la sécurité des systèmes d'information afin que ces questions soient portées publiquement** et qu'elles ne soient plus réservées uniquement à un petit cercle de spécialistes.

Comme on l'a vu aux **Etats-Unis**, le Président Barack Obama a fait de la cybersécurité une priorité de son mandat et il s'est fortement investi sur ce sujet en consacrant plusieurs discours aux enjeux liés à la sécurité des systèmes d'information.

De même, **au Royaume-Uni**, le Premier ministre M. David Cameron est également intervenu à de nombreuses reprises sur ce thème. Il a notamment reçu personnellement les représentants des principaux opérateurs d'importance vitale pour les inciter à renforcer la coopération entre le secteur public et le secteur privé et il a pris l'initiative de réunir une grande conférence internationale à Londres consacrée à la cybersécurité, en novembre dernier.

Pour votre rapporteur, l'importance des enjeux liés à la protection et la défense des systèmes d'information justifie que ces questions fassent l'objet d'**une véritable priorité nationale, portée au plus haut niveau de l'Etat.**

C. POUR UNE VÉRITABLE POLITIQUE DE CYBERSÉCURITÉ DE L'UNION EUROPÉENNE

Comme on l'a vu précédemment, l'Union européenne a un rôle important à jouer en matière de protection des systèmes d'information, car une grande partie des règles dans ce domaine relèvent de ses compétences.

Or, l'Union européenne n'a pas encore pris réellement la mesure des enjeux liés à la protection des systèmes d'information.

Avant toute chose, il semble indispensable que **l'Union européenne se dote d'une véritable stratégie européenne qui englobe l'ensemble des questions liées au cyberespace,** qu'il s'agisse de la sécurité et de la résilience des systèmes d'information, en particulier des opérateurs d'infrastructures d'informations critiques, de la cyberdéfense, de la lutte contre la cybercriminalité ou encore des enjeux liés à la liberté d'expression, aux effets d'Internet sur le développement économique ou encore à la gouvernance d'Internet.

Une telle stratégie devrait notamment permettre d'assurer une meilleure coordination entre les différentes entités chargées de ces questions à l'échelle européenne et une plus grande cohérence d'ensemble.

Afin de lui conférer un poids politique suffisant, cette stratégie devrait, aux yeux de votre rapporteur, être adoptée par le Conseil européen.

Si la protection des systèmes d'information doit demeurer avant tout une compétence nationale, car elle touche directement à la souveraineté de chaque Etat, l'Union européenne pourrait intervenir dans deux domaines :

D'une part, concernant l'aspect préventif, en soutenant les mesures de sécurité, de confiance et de résilience en Europe. D'autre part, s'agissant de l'aspect défensif, en encourageant les capacités en matière de cybersécurité au niveau de chaque Etat membre et au sein des institutions européennes.

1. Encourager la sécurité, la confiance et la résilience à l'échelle européenne

L'Union européenne se doit d'abord d'encourager **le développement de mesures de sécurité, de confiance et de résilience à l'échelle européenne.**

Ainsi, l'Union européenne pourrait jouer un rôle plus actif en matière de normes, car une grande partie des règles applicables aux opérateurs de réseaux relèvent de ses compétences.

Dans le cadre du « Paquet télécom », l'Union européenne a imposé aux opérateurs de télécommunications la mise en œuvre de mesures minimales en matière de protection des systèmes d'information. Une disposition a également été introduite afin de contraindre les opérateurs de

télécommunications à notifier aux autorités nationales compétentes toute atteinte à la sécurité ou à la perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.

Il semble souhaitable d'étendre ces mesures et cette déclaration obligatoire d'incident à d'autres secteurs.

Plus généralement, l'Union européenne devrait définir des règles ou garanties minimales à l'échelle européenne en matière de sécurité informatique applicables à l'ensemble des acteurs et des réseaux concernés afin d'en accroître très fortement la résilience.

L'agence européenne ENISA a certes publié des recommandations ou des guides de « bonnes pratiques » concernant les règles minimales de sécurité informatique, mais ces instruments n'ont pas de portée contraignante.

On pourrait donc s'appuyer sur la directive cadre du « Paquet télécom », qui impose aux Etats membres la mise en œuvre de mesures minimales en matière de protection des systèmes d'information, pour renforcer ces mesures en fixant au niveau européen de véritables règles ou garanties minimales en matière de sécurité informatique.

L'Union européenne pourrait aussi développer la coopération et le travail en commun entre les différents acteurs, c'est-à-dire les Etats, les opérateurs, les régulateurs et les industriels.

Ainsi, on pourrait mettre en place au sein de l'Union des mesures visant à soutenir le secteur privé afin d'améliorer la prise en compte de la sécurité dans les produits et services informatiques. A cet égard, la sécurité informatique devrait occuper une place plus importante dans les travaux de standardisation et de certification à l'échelle européenne, en particulier concernant les équipements utilisés dans les réseaux de communications électroniques, mais aussi, plus largement, de l'ensemble des produits. Le développement des activités de sensibilisation auprès des entreprises européennes comme des consommateurs mériterait aussi d'être encouragé. Des mesures de nature à renforcer la confiance dans la chaîne d'approvisionnement des éléments d'importance critique devraient également être étudiées.

Pour votre rapporteur, l'Union européenne devrait aussi encourager une politique industrielle volontariste à l'échelle européenne, en soutenant les entreprises, notamment les PME, qui proposent des produits ou des conseils en matière de sécurité informatique.

L'Union européenne pourrait ainsi favoriser l'émergence de « champions » nationaux ou européens.

Pourquoi ne pas envisager un *« Small business Act »* à l'échelle européenne, pour soutenir les PME qui proposent des produits ou des services importants du point de vue de la sécurité informatique ?

Plus largement, l'Union européenne devrait soutenir davantage l'industrie européenne des technologies de l'information et de la communication.

Le secteur des technologies de l'information et de la communication présente une importance cruciale pour l'Europe, à la fois du point de vue stratégique, mais aussi économique.

Ce secteur est aujourd'hui dominé par des grandes entreprises nord-américaines mais aussi, de plus en plus, menacé par la concurrence d'entreprises asiatiques, chinoises ou coréennes. Quant à l'industrie européenne, elle a pratiquement disparu de ce secteur et il ne subsiste encore en Europe que quelques niches, assez fragiles.

Or, les grands équipements informatiques, à l'image des « routeurs de cœur de réseaux » qui gèrent les flux de communication, présentent un caractère hautement sensible du point de vue de la sécurité nationale.

Compte tenu des montants financiers en jeu, seule une coopération industrielle à l'échelle européenne permettrait aux pays européens de ne pas dépendre uniquement d'équipements d'origine américaine ou asiatique.

Pourquoi ne pas utiliser les fonds structurels et les fonds de cohésion pour renforcer la sécurité informatique des infrastructures de télécommunications en Europe ?

Votre rapporteur appelle donc de ses vœux une véritable politique industrielle à l'échelle européenne dans ce secteur sensible.

Rendre l'action de l'Union européenne en matière de recherche et de développement plus efficace constitue aussi une priorité.

Dans le cadre du programme cadre de recherche et de développement (PCRD) ou du programme compétitivité et innovation (CIP), l'Union européenne dispose certes de financements importants destinés à soutenir la recherche et l'innovation dans le domaine des technologies de l'information et de la communication.

Toutefois, ces instruments souffrent des défauts souvent constatés à propos de la plupart des programmes européens : absence de véritables priorités, dispersion des moyens, difficulté à trouver des co-financements, longueur et lourdeur de la procédure et de la gestion, etc.

Il convient donc d'améliorer l'efficacité et la coordination des programmes européens afin de permettre d'encourager la recherche et le développement en matière de sécurité des systèmes d'information et, plus largement, dans le domaine des technologies de l'information et de la communication.

Enfin, **l'Union européenne a un rôle important à jouer en matière de sensibilisation de tous les acteurs, qu'il s'agisse des Etats, des entreprises, des opérateurs et industriels ou des citoyens européens.**

2. Renforcer les capacités de cyberdéfense des Etats membres et des institutions européennes

L'Union européenne devrait aussi encourager la mise en place de capacités de cyberdéfense au sein des différents Etats-membres et renforcer la protection de ses propres systèmes d'information et de communication

Ainsi, l'Union européenne devrait se fixer comme objectif d'accélérer le développement des capacités de cybersécurité au sein des différents Etats membres, en particulier concernant les pays les moins avancés dans le domaine de la protection des systèmes d'information, et renforcer la coopération entre les Etats, notamment en matière de préparation et de réponse aux crises.

Actuellement, de nombreux pays européens restent encore insuffisamment sensibilisés aux menaces pesant à l'encontre des systèmes d'information.

La compétence opérationnelle de réponse aux incidents de sécurité informatique relevant entièrement de la compétence nationale, le rôle de l'Union européenne devrait principalement consister à encourager le développement de capacités nationales, en incitant par exemple les Etats à mettre en place des autorités nationales chargées de la protection des systèmes d'information ou à créer un CERT gouvernemental.

Les institutions européennes, et l'ENISA en particulier, ont également un rôle important à jouer en matière d'analyse des risques, d'échanges d'information ou pour l'organisation d'exercices à l'échelle européenne de crises cyber. Ainsi, l'ENISA pourrait apporter un soutien à la mise en place d'un réseau fonctionnel de CERT nationaux en Europe bénéficiant de moyens de communication sécurisés.

Il paraît également nécessaire de renforcer de manière significative la protection des systèmes d'information des institutions européennes et des différentes structures qui leur sont rattachées.

Les capacités de l'Union européenne devraient être accrues afin que l'Europe soit en mesure d'assurer une protection effective de ses propres réseaux et systèmes d'information et une veille opérationnelle.

Enfin, **l'Union européenne pourrait s'affirmer sur ces questions comme un acteur au niveau international face aux Etats-Unis, à la Chine, à la Russie ou aux autres puissances émergentes**.

Il existe déjà un groupe de travail conjoint entre l'Union européenne et les Etats-Unis, qui permet d'échanger avec nos amis américains sur différents sujets, comme la lutte contre la cybercriminalité. On peut regretter cependant que les Etats membres ne soient pas davantage associés à ce groupe de travail, alors que ces sujets relèvent avant tout de leurs compétences.

Plus généralement, la place de l'Union européenne dans les différentes enceintes internationales qui traitent de ces aspects, à l'image des Nations Unies ou de l'Union internationale des télécommunications, mériterait d'être renforcée car cela permettrait aux pays européens de « parler d'une seule voix » face aux Etats-Unis ou aux puissances émergentes.

Pourquoi ne pas encourager aussi l'Union européenne à favoriser un dialogue avec certains pays, comme la Chine ou la Russie, sur ces sujets ?

3. Un enjeu majeur : Pour une interdiction totale sur le territoire européen des « routeurs de cœur de réseaux » et autres équipements informatiques sensibles d'origine chinoise

Selon un article récent du *Financial Times*[1], la Commission européenne serait sur le point de lancer une procédure d'infraction pour non respect des règles européennes de la concurrence à l'encontre des entreprises chinoises Huawei et ZTE, qui proposent des grands équipements informatiques, à l'image des « routeurs de cœur de réseaux ». La Commission européenne soupçonne, en effet, ces entreprises de bénéficier de subventions du gouvernement chinois et de vendre leurs produits en dessous des coûts de production.

Qu'est-ce qu'un « routeur » ?

La connexion d'un site à l'Internet ou à des réseaux repose sur les « routeurs ». Les « routeurs de cœur de réseaux » sont des grands équipements d'interconnexion de réseaux informatiques utilisés par les opérateurs de télécommunications qui permettent d'assurer le flux des paquets de données entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

La fiabilité des « routeurs » doit être à toute épreuve, leur sécurisation renforcée et leur surveillance assurée. En effet, toute perturbation du « routeur » peut isoler un site du reste du monde ou engendrer une compromission de l'intégralité des données transitant par cet équipement.

Actuellement, le marché mondial est nettement dominé par des entreprises américaines, comme Cisco, mais on relève une forte volonté de pénétration des entreprises chinoises Huawei et ZTE, sur le marché américain et européen.

Huawei a ainsi investi significativement le marché britannique des télécommunications. Elle a passé un contrat avec l'opérateur de téléphonie mobile Telefonica pour planifier, implémenter et gérer la majorité de leur activité. Pour sa part, ZTE a présenté un nouvel équipement pour réseaux en fibres optiques, capable de supporter un très haut débit et souhaite figurer parmi les premiers fabricants d'ordiphones au monde.

---

[1] *Financial Times, "Beijing Faces Brussels Action on Telecoms Aid", 29 mai 2012*

Si une telle procédure d'infraction serait principalement motivée par le respect des règles européennes de la concurrence et les soupçons pesant sur ces deux entreprises chinoises en matière de concurrence déloyale, elle ne serait toutefois pas étrangère à des préoccupations liées à la sécurité nationale.

Selon les informations recueillies par votre rapporteur lors de ses entretiens à Bruxelles, cette question ferait actuellement l'objet de fortes discussions au niveau européen, en raison des divergences entre les Etats membres et au sein de la Commission européenne et des fortes pressions des industriels et des opérateurs de télécommunications, dont certains seraient sensibles aux avantages économiques de ces équipements proposés par les entreprises chinoises à moindre coûts.

Or, **les « routeurs de réseaux » sont des équipements hautement sensibles du point de vue de la sécurité des systèmes d'information**.

Rien n'empêcherait, en effet, un pays producteur de ce type d'équipements d'y placer un dispositif de surveillance, d'interception, voire un système permettant d'interrompre à tout moment l'ensemble des flux de communication.

Le fait de placer un tel dispositif de surveillance directement au cœur du « routeur de réseaux » rendrait ce dispositif presque totalement « invisible » et indétectable. Et il n'est pas indifférent de savoir que de forts soupçons pèsent sur la Chine en matière de provenance des attaques informatiques, notamment à des fins d'espionnage économique.

Aux Etats-Unis, les autorités ont d'ailleurs pris ces dernières années plusieurs mesures afin de limiter la pénétration des équipementiers chinois Huawei et ZTE sur le marché américain pour des raisons liées à la sécurité nationale.

Ainsi, dès 2008, le gouvernement américain a décidé de bloquer la vente de la société américaine « 3Com » à Huawei pour des motifs de sécurité nationale. En 2011, les autorités américaines ont également découragé l'opérateur « Sprint Nextel » d'utiliser des composants fabriqués par Huawei pour la construction de son réseau 4G pour des raisons identiques.

Comme l'a déclaré le porte-parole du département du commerce américain, *« Huawei ne fera pas partie des constructeurs du réseau sans fil d'urgence américain à cause d'interrogations du gouvernement américain au sujet de la sécurité nationale »*.

Les autorités américaines soupçonnent que les puces, routeurs et autres équipements informatiques chinois soient équipés de « portes dérobées » permettant au gouvernement chinois d'accéder à des informations sensibles transitant par ces équipements. Elles s'appuient sur un rapport du Pentagone, qui indique que *« Huawei continue à maintenir d'étroites relations avec l'armée de libération du peuple chinoise »*.

D'après un récent article du *Wall Street Journal*[1], plusieurs parlementaires américains, membres de la commission du renseignement de la Chambre des représentants, ont d'ailleurs lancé une enquête sur les activités de Huawei et de ZTE aux Etats-Unis et les relations de ces sociétés avec le gouvernement chinois et le comité central du parti communiste chinois, dans le cadre des soupçons d'espionnage en provenance de Chine.

Comme l'a indiqué l'un de ces parlementaires, M. Dutch Ruppersberger : *« nous sommes très inquiets par les attaques informatiques menées par le gouvernement chinois à l'encontre de nos réseaux nationaux. Notre inquiétude porte sur la possibilité pour le gouvernement chinois d'accéder par l'intermédiaire des équipements Huawei ou ZTE aux conversations téléphoniques ou aux e-mails, et qu'il puisse interrompre ou détruire les systèmes de communications ».*

De même, **en Australie**, les autorités ont interdit aux opérateurs de télécommunications l'utilisation de « routeurs chinois » pour équiper les réseaux sur leur territoire en raison des soupçons de cyberattaques en provenance de Chine[2]. Comme l'a déclaré le porte-parole du gouvernement, *« nous avons la responsabilité de faire le maximum pour protéger l'intégrité des réseaux nationaux et des informations qui y circulent ».*

Selon un autre article[3], ces soupçons semblent avoir été confirmés de manière involontaire par les représentants de l'entreprise chinoise Huawei eux-mêmes, lors d'une présentation devant une conférence organisée à Dubaï en février dernier.

En effet, dans leur présentation, ils auraient indiqué que, pour mieux assurer la sécurisation des flux de ses clients, Huawei *« analysait »* (grâce aux techniques dites de *« deep packet inspection »* ou DPI), l'ensemble des flux de communications (courriers électroniques, conversations téléphoniques, etc.) qui transitaient par ses équipements.

Si les représentants de l'entreprise voulaient démontrer avant tout les capacités de leurs « routeurs » en matière de détection de « logiciels malveillants », ils ont ainsi confirmé, comme cela a d'ailleurs été relevé par plusieurs participants à cette conférence, les capacités potentielles de ces « routeurs » à analyser, intercepter et extraire des données sensibles, voire à les altérer ou les détruire.

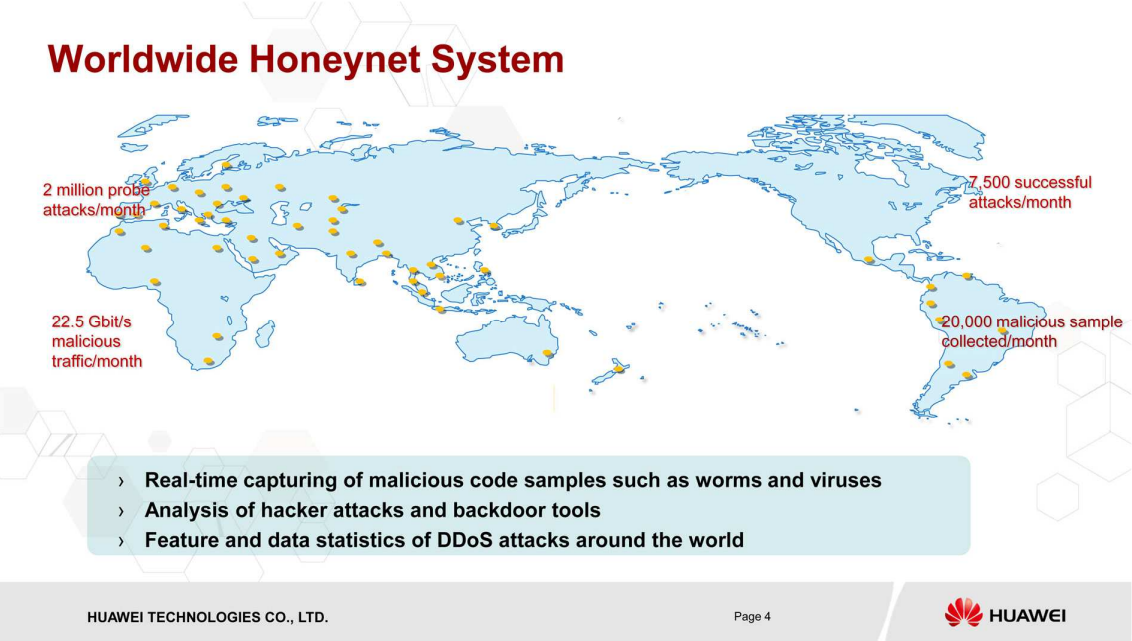
Il est donc crucial que l'Union européenne adopte une position ferme d'une totale interdiction concernant le déploiement et l'utilisation des « routeurs » chinois sur le territoire européen, ou d'autres grands équipements informatiques d'origine chinoise ne présentant pas toutes les garanties en matière de sécurité informatique.

---

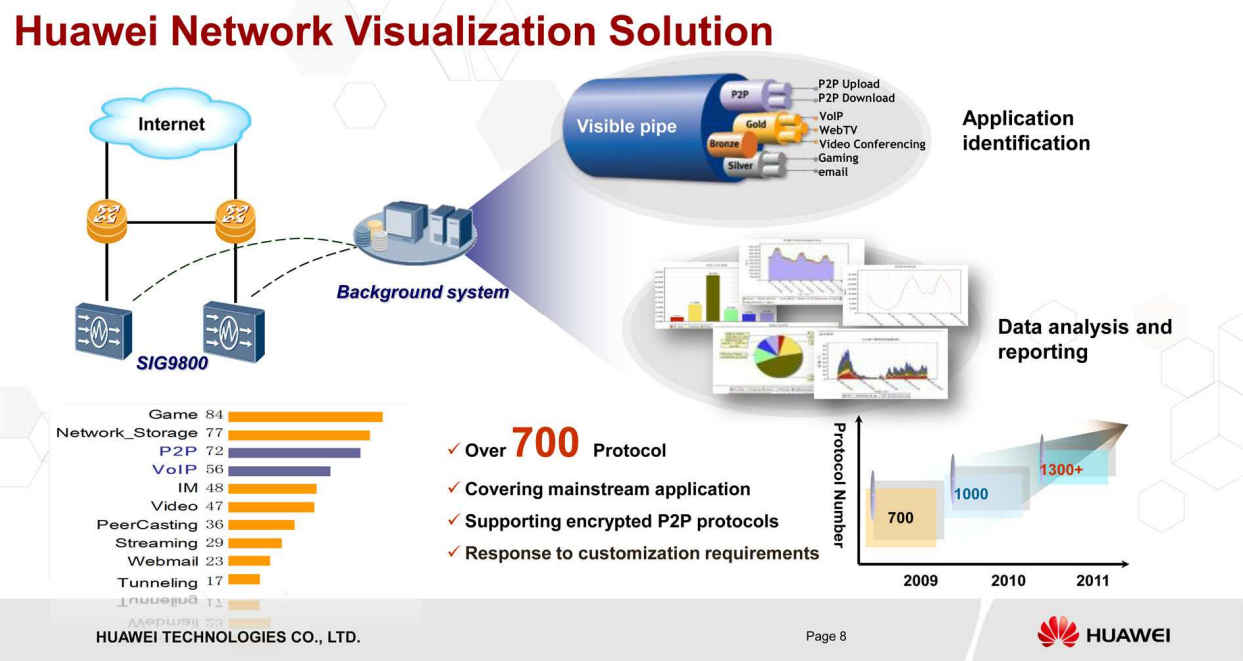
[1] *The Wall Street Journal,* « China Firms Under Fire », *13 juin 2012*
[2] *The Australian Financial Review, « China's Huawei banned from NBN », 24 mars 2012*
[3] *WND, « China tech company brags : we hacked U.S. Telecoms », 6/14/2012*

A terme, votre rapporteur considère qu'il serait souhaitable de lancer une coopération industrielle entre la France et l'Allemagne ou à l'échelle européenne afin de développer des *« routeurs de cœur de réseaux »* ou d'autres grands équipements informatiques européens, et de ne plus dépendre uniquement de produits américains ou asiatiques.

Les illustrations d'un « routeur de cœur de réseau »



Le réseau mondial d'implantation de routeurs et d'équipements de Huawei



Le mode d'analyse du trafic par Huawei

CONCLUSION

Face au rôle central des systèmes d'information et de communication et à l'extrême dépendance de nos sociétés, qui ne pourra que s'accroître à l'avenir avec le développement des nouvelles technologies d'information et de télécommunications, leur interconnexion croissante et la généralisation de l'utilisation dans notre vie quotidienne d'objets connectés, le renforcement de la protection et de la défense des systèmes d'information représente **un enjeu majeur de sécurité nationale**.

Certes, il ne s'agit pas de prétendre à une protection absolue. Cela serait assez illusoire. Le propre des attaques informatiques est d'exploiter les failles, de se porter là où les parades n'ont pas encore été mises en place. A l'image de la course perpétuelle entre la lance et le bouclier, les techniques évoluent sans cesse et il n'existe pas de sécurité absolue dans le « cyberespace ».

Mais on peut améliorer la sécurité des réseaux et des infrastructures les plus sensibles, mettre en place des systèmes d'analyse permettant de détecter les attaques, un ensemble de mesures pour être capable de faire face à une crise et de rétablir les systèmes, sensibiliser les concepteurs, les gestionnaires et les utilisateurs des systèmes d'information à adopter des règles d'« hygiène » élémentaires et renforcer leur résilience.

Malgré une prise de conscience tardive, notamment par rapport aux Etats-Unis et à nos principaux alliés européens, **la France a réalisé**, grâce à l'impulsion donnée par le Livre blanc sur la défense et la sécurité nationale de 2008, **d'importants efforts dans ce domaine**. Une agence nationale de la sécurité des systèmes d'information a été instituée et notre pays s'est doté d'une stratégie de cyberdéfense.

Pour autant, face à la forte augmentation et à la diversification des attaques informatiques dirigées contre notre pays et nos intérêts économiques ou stratégiques, **beaucoup reste encore à faire** pour renforcer la prise en compte des enjeux liés à la sécurité des systèmes d'information au sein de l'Etat, des entreprises ou des opérateurs d'importance vitale et sensibiliser davantage les utilisateurs à ces questions.

Aux yeux de votre rapporteur, compte tenu de l'importance des enjeux, le renforcement de la protection et de la défense des systèmes d'information devrait faire l'objet d'**une priorité nationale**, **portée au plus haut niveau de l'Etat**, et d'**une véritable stratégie de l'Union européenne**. Soucieux que les orientations qui figurent dans ce rapport puissent être reprises ou du moins servir d'inspiration, notamment dans le contexte du nouveau Livre blanc sur la défense et la sécurité nationale et de la future loi de programmation militaire, votre rapporteur a pensé utile de présenter ses préconisations sous la forme de **10 priorités**, assorties de **50 recommandations concrètes**.

LISTE DES 50 RECOMMANDATIONS

1°) Au niveau de l'Etat

Recommandation n°1 : Faire de la cyberdéfense et de la protection des systèmes d'information une priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. Rendre la politique nationale plus « lisible ».

➢ ***L'ANSSI :***

Recommandation n°2 : Conforter le modèle français reposant sur l'ANSSI tout en développant ses relations avec les armées, la DGA et les services spécialisés. Poursuivre, voire amplifier, l'augmentation des effectifs et des moyens de l'ANSSI dans les prochaines années, au moyen d'un programme pluriannuel, réévalué régulièrement

Recommandation n°3 : Introduire des modifications législatives pour donner les moyens à l'ANSSI, aux armées et aux services spécialisés d'exercer leurs missions, notamment en autorisant la rétroconception à des fins de sécurité, en prévoyant la possibilité de procéder à l'analyse de comportement des codes malveillants, la possibilité de mettre en place des dispositifs permettant de suivre les actions d'un attaquant ou encore l'identification et la collecte de vulnérabilités des outils utilisés par l'attaquant.

Recommandation n°4 : Donner réellement à l'ANSSI les pouvoirs afférents à son rôle d'« autorité nationale » en lui conférant un véritable pouvoir d'imposition en ce qui concerne la politique de sécurité des systèmes d'information des acteurs publics et des opérateurs d'importance vitale

Recommandation n°5 : Développer le rôle de l'ANSSI en matière de « labellisation » et de « certification » de produits sécurisés et lui donner les moyens de soutenir les services informatiques des administrations pour l'acquisition et l'intégration de ces produits, ainsi que pour l'intégration des produits agréés et qualifiés et pour l'intégration de systèmes d'exploitation durcis

Recommandation n°6 : Instaurer une politique des ressources humaines au sein des services de l'Etat concernant les spécialistes de la sécurité informatique en encourageant le recrutement, la formation, les mobilités et le déroulement des carrières au sein et entre les services de l'Etat

➢ ***Le ministère de la Défense :***

Recommandation n°7 : Poursuivre et amplifier les moyens techniques et humains consacrés à la cyberdéfense au sein des armées, de la DGA et des services spécialisés. Promouvoir une « cyber réserve » au sein de la réserve citoyenne et opérationnelle.

Recommandation n°8 : Conforter et approfondir la nouvelle organisation de cybersécurité mise en place au sein du ministère de la défense en renforçant le rôle du fonctionnaire de la sécurité des systèmes d'information (FSSI) et en révisant son positionnement au sein de la Direction générale des systèmes d'information et de communication (DGSIC)

Recommandation n°9 : Encourager et soutenir le rôle de la DGA en matière de conception et de certification de produits de haut niveau de sécurité pour les besoins militaires, civils et interministériels

Recommandation n°10 : Poursuivre le développement de capacités offensives au sein des armées et des services spécialisés. Renforcer le suivi de ces capacités par la délégation parlementaire au renseignement. S'interroger sur la pertinence d'un discours public, voire d'une doctrine publique, sur les capacités offensives

➢ L'ensemble des ministères :

Recommandation n°11 : Faire de la protection des systèmes d'information une véritable priorité prise en compte dans l'action de chaque ministère, réserver un pourcentage significatif du montant des projets à la sécurité informatique

Recommandation n°12 : Rendre obligatoire pour chaque ministère la tenue d'une cartographie à jour de son propre réseau et de son système d'information. Dans l'attente de l'édification du Réseau Interministériel de l'Etat (RIE), réduire le nombre de passerelles entre les réseaux des ministères et l'Internet et développer les systèmes de surveillance de ces passerelles permettant de détecter les attaques

Recommandation n°13 : Rehausser l'autorité et le rôle des fonctionnaires de la sécurité des systèmes d'information (FSSI) afin qu'ils deviennent au sein de chaque ministère de véritables directeurs ou secrétaires généraux de la sécurité et de la défense des systèmes d'information (DSSI ou SGSSI) auxquels devront être soumis pour avis les projets informatiques des administrations

Recommandation n°14 : Renforcer les effectifs et les moyens de la direction interministérielle des systèmes d'information et de communication de l'Etat (DISIC) en matière de sécurité des systèmes d'information et poursuivre la mise en place du Réseau Interministériel de l'Etat

Recommandation n°15 : Accroître les efforts de sensibilisation des personnels des administrations, à tous les échelons, notamment par la signature de charte d'utilisation des systèmes d'information

Recommandation n°16 : Instituer un pôle juridictionnel spécialisé à compétence nationale, sur le modèle du pôle de lutte contre le terrorisme ou du pôle financier, pour réprimer les atteintes graves aux systèmes d'information. Former les magistrats de ce pôle

2°) Concernant les entreprises et les opérateurs d'importance vitale

➢ ***Les entreprises :***

Recommandation n°17 : Rendre obligatoire une déclaration d'incident à l'ANSSI en cas d'attaque importante contre les systèmes d'information et encourager les mesures de protection par des mesures incitatives

Recommandation n°18 : Faire de la protection des systèmes d'information une véritable priorité en matière de management des entreprises en sensibilisant les dirigeants des entreprises et en rehaussant le niveau hiérarchique et le rôle des responsables de la sécurité informatique

Recommandation n°19 : Engager une réflexion avec les compagnies d'assurance sur la prise en charge des opérations de traitement d'une cyberattaque moyennant un certain niveau de sécurité initial et la réalisation d'un audit annuel

Recommandation n°20 : Renforcer les échanges entre l'ANSSI et les entreprises spécialisées dans la conception de produits ou de services de sécurité informatique en mettant en place un réseau de prestataires de confiance

Recommandation n°21 : Encourager par une politique industrielle volontariste le tissu industriel des entreprises françaises, notamment des PME, spécialisées dans la conception de certains produits ou services importants pour la sécurité informatique

Recommandation n°22 : Encourager et développer le rôle des sociétés privées de conseil et d'assistance en matière de sécurité informatique, par un système d'agrément ou de label, des modifications législatives et des mesures incitatives

Recommandation n°23 : Améliorer et renforcer le soutien à l'export des entreprises françaises proposant des produits de sécurité informatique

➢ ***Les opérateurs d'importance vitale :***

Recommandation n°24 : Rendre obligatoire pour les opérateurs d'importance vitale une déclaration d'incident à l'ANSSI dès la détection d'un incident informatique susceptible de relever d'une attaque contre les systèmes d'information et pouvant porter atteinte au patrimoine informationnel ou à l'exercice des métiers de l'opérateur, et encourager les mesures de protection par des mesures incitatives

Recommandation n°25 : Réduire le nombre de passerelles entre les réseaux et l'Internet et introduire un système de surveillance des flux permettant de déceler les attaques informatiques, agréé par l'ANSSI et favoriser le groupement d'opérateurs d'importance vitale autour de système de détection partagés opérationnels 24/24

Recommandation n°26 : Encourager la coopération et les échanges entre l'ANSSI et les opérateurs d'importance vitale dans le cadre d'une démarche sectorielle. Rendre obligatoire le maintien d'une cartographie à jour des systèmes d'information, un audit annuel en matière de sécurité des systèmes d'information, ainsi qu'une déclaration à l'ANSSI de systèmes de contrôle des processus ou des automates industriels (SCADA) connectés à l'Internet

➢ ***Les universités et centres de recherches***

Recommandation n°27 : Encourager la formation d'ingénieurs spécialisés dans la protection des systèmes d'information et prévoir un module consacré à la protection des systèmes d'information dans toutes les formations d'ingénieurs, dans les grandes écoles d'ingénieurs, les universités et l'enseignement technique. Inclure une sensibilisation obligatoire dans les écoles formant les cadres de l'administration (comme l'ENA par exemple) et proposer une telle sensibilisation aux formations de management destinées aux entreprises

Recommandation n°28 : Accentuer la recherche et développement en matière de sécurité des systèmes d'information et renforcer les relations des acteurs publics avec les universités et les centres de recherche

➢ ***Le grand public***

Recommandation n°29 : Améliorer la sensibilisation du public par un plan de communication inspiré du plan de prévention de la sécurité routière

3°) Concernant les relations internationales

➢ ***Les échanges bilatéraux***

Recommandation n°30 : Poursuivre et développer la coopération en termes quantitatifs et qualitatifs avec les CERT gouvernementaux et militaires

Recommandation n°31 : Poursuivre et renforcer la coopération bilatérale avec le Royaume-Uni, autour des capacités techniques et opérationnelles, notamment au profit du domaine militaire et de la sécurité des opérateurs d'infrastructures vitales communs

Recommandation n°32 : Poursuivre et renforcer la coopération bilatérale avec l'Allemagne, notamment sur les projets industriels et de recherche conjoints, ainsi qu'au profit de la sécurité des opérateurs d'infrastructures vitales communs

Recommandation n°33 : Développer notre influence en renforçant les relations bilatérales avec des pays ayant mis en place, ou souhaitant mettre en place, une organisation nationale de gestion de la cybersécurité, afin de promouvoir le modèle français de gouvernance en matière de cybersécurité, de promouvoir l'industrie française, et de développer une communauté de vue la plus large possible sur les questions internationales en matière de cybersécurité afin de peser plus efficacement dans les enceintes internationales

Recommandation n°34 : Favoriser le dialogue : mettre en place des dialogues stratégiques bilatéraux avec les pays pouvant jouer un rôle particulier en matière de cyberattaques à l'encontre de nos intérêts nationaux, afin de développer progressivement la confiance, via l'amélioration de la connaissance mutuelle de nos organisations et de nos postures stratégiques, ainsi que sur l'entraide internationale en matière de cybercriminalité

- ***Les enceintes multilatérales***

L'OTAN :

Recommandation n°35 : Concentrer le rôle de l'OTAN sur la protection des systèmes d'information et de communication propres à l'Alliance et poursuivre le développement de capacités opérationnelles de l'OTAN (centre opérationnel 24h/24 7jours/7)

Recommandation n°36 : Encourager la coopération OTAN/Union européenne, en s'appuyant sur la complémentarité de leurs approches, notamment en matière d'infrastructures critiques

Recommandation n°37 : Poursuivre les discussions afin d'élaborer une doctrine au sein de l'OTAN (recours à l'article V en cas de cyberattaque)

Recommandation n°38 : Prévoir une présence française au sein du centre d'excellence de Tallinn

L'Union européenne :

Recommandation n°39 : Promouvoir une véritable stratégie globale européenne en matière de protection des systèmes d'information au sein de l'Union européenne. Rendre l'action de l'UE plus « lisible ».

Recommandation n°40 : Réformer fondamentalement l'agence européenne ENISA afin d'en faire véritablement un outil de soutien réellement efficace aux Etats membres

Recommandation n°41 : Inciter l'Union européenne à assurer la protection de ses propres réseaux en renforçant le rôle du CERT des institutions de l'Union européenne, notamment auprès des organismes dépendants de l'Union européenne

Recommandation n°42 : Renforcer la coopération industrielle européenne en matière de conception de produits informatiques ou de sécurité informatique, et soutenir l'industrie européenne des technologies de l'information et de la communication afin d'en assurer la compétitivité et la pérennité, notamment grâce à des financements ou des mécanismes innovants (programme compétitivité et innovation par exemple) en priorité dans le domaine des télécommunications (routeurs et équipements cœur de réseau) mais également dans des domaines comme l'électronique (processeurs, PC), les systèmes d'exploitation ou les environnements sécurisés. Encourager la recherche au niveau européen par le biais du programme cadre de recherche et développement.

Recommandation n°43 : Développer le rôle de l'Union européenne en matière de normes juridiques afin de renforcer la protection des systèmes d'information des entreprises et des infrastructures critiques au niveau européen, notamment la protection des infrastructures critiques européennes et les infrastructures d'information (en posant notamment des garanties minimales à l'échelle européenne en matière de sécurité informatique).

Recommandation n°44 : Interdire sur le territoire national et européen le déploiement et l'utilisation de « routeurs » ou d'équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les « routeurs » ou d'autres équipements informatiques d'origine chinoise

L'ONU :

Recommandation n°45 : Défendre l'idée d'un code de bonne conduite ou de mesures de confiance au niveau international et séparant clairement les éléments liés aux contenants techniques de ceux liés aux informations, plutôt qu'un traité international ou d'un texte international juridiquement contraignant

Recommandation n°46 : Encourager un dialogue franc et ouvert avec la Chine et la Russie sur ces sujets

L'UIT :

Recommandation n°47 : Encourager le rôle d'aide au développement de capacités nationales, notamment des pays en voie de développement, de l'UIT, tout en s'opposant à la reconnaissance d'un fondement juridiquement contraignant à l'action de l'UIT sur la cybersécurité (hors du traité des télécommunications) et à un rôle opérationnel en ce domaine

L'OCDE :

Recommandation n°48 : Utiliser l'OCDE pour s'informer sur les visions promues par les autres Etats et comme enceinte d'influence pour évaluer et promouvoir les visions développées au niveau national

L'OSCE :

Recommandation n°49 : Encourager au sein de l'OSCE le développement et l'expérimentation de mesures favorisant la confiance avec la Russie, en parallèle des travaux menés à l'ONU

➢ ***L'Influence sur les standards techniques et la participation dans les enceintes de normalisation :***

Recommandation n°50 : Engager une activité de veille sur les enjeux de sécurité des systèmes d'information et de cybersécurité soulevés par les standards techniques en cours de développement, au sein ou en dehors de groupes de normalisation, afin de les identifier précocement, s'assurer du développement de positions nationales, et les faire porter par les représentants français ou nos alliés, publics ou privés

EXAMEN EN COMMISSION

La commission des affaires étrangères, de la défense et des forces armées a examiné le présent rapport d'information lors de sa séance du 18 juillet 2012.

M. Jean-Louis Carrère, président – Après avoir examiné les questions relatives à l'avenir des forces nucléaires, aux capacités industrielles souveraines, au format des forces après 2014 et à la « maritimisation », nous allons procéder maintenant à l'examen du dernier des cinq rapports d'information qui s'inscrivent dans le cadre des travaux de notre commission lancés dans l'optique de l'élaboration du nouveau Livre blanc sur la défense et la sécurité nationale. Ce rapport, présenté par notre collègue M. Jean-Marie Bockel, est consacré à un sujet assez peu connu, mais qui prend aujourd'hui une importance croissante : le thème de la cyberdéfense. Je laisse donc la parole à notre collègue.

M. Jean-Marie Bockel, rapporteur – Notre commission avait déjà adopté, en juillet 2008, un rapport d'information sur la cyberdéfense, présenté par notre ancien collègue M. Roger Romani.

Beaucoup de choses se sont passées depuis quatre ans.

C'est la raison pour laquelle notre commission a souhaité faire à nouveau le point sur cette question et m'a confié ce rapport d'information, notamment dans l'optique de l'élaboration du nouveau Livre blanc sur la défense et la sécurité nationale.

Depuis octobre, j'ai eu de nombreux entretiens avec les principaux responsables chargés de la protection des systèmes d'information au sein des services de l'Etat et des armées.

J'ai également rencontré, en tête-à-tête, le chef d'Etat major particulier du Président de la République, ainsi que les représentants des services de renseignement.

J'ai aussi eu des entretiens avec des dirigeants d'entreprises, dont certaines ont été victimes d'attaques informatiques, à l'image d'AREVA, et même avec ceux qu'on appelle des « pirates informatiques ».

Afin d'avoir une vue comparative, je me suis rendu à Londres et à Berlin, à Tallin et à Washington, ainsi qu'à Bruxelles au siège de l'OTAN et auprès des institutions de l'Union européenne.

Je vous avais d'ailleurs présenté un premier rapport d'étape en février dernier.

Aujourd'hui, je voudrais vous présenter les principales conclusions de mon rapport et vous proposer d'adopter un certain nombre de recommandations.

Mais, tout d'abord, que faut-il entendre par « cyberdéfense » ?

On parle souvent indistinctement de « cybercriminalité », de « cyber menaces », de « cyber attaques » ou de « cyber guerres ». Il faut bien comprendre que les méthodes utilisées à des fins de fraude ou d'escroquerie sur Internet peuvent l'être aussi, à une échelle plus vaste, contre la sécurité et les intérêts essentiels de la Nation.

C'est le cas avec la pénétration de réseaux en vue d'accéder à des informations sensibles ou avec des attaques informatiques visant à perturber ou à détruire des sites largement utilisés dans la vie courante.

Dans mon esprit, la cyberdéfense se distingue de la lutte contre la cybercriminalité. Elle recouvre la politique mise en place par l'Etat pour protéger activement des réseaux et des systèmes d'information essentiels à la vie et à la souveraineté du pays.

Pourquoi s'intéresser de nouveau à cette question ?

Avec le développement de l'Internet, les systèmes d'information constituent désormais les véritables « centres nerveux » de nos sociétés, sans lesquels elles ne pourraient plus fonctionner. Or, depuis les attaques informatiques massives qui ont frappé l'Estonie en avril 2007, la menace s'est concrétisée et accentuée.

Il ne se passe pratiquement pas une semaine sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de grands organismes publics ou privés.

La France n'est pas épargnée par ce phénomène.

Comme me l'ont confirmé les représentants des organismes chargés de la protection des systèmes d'information, nos administrations, nos entreprises ou nos opérateurs d'importance vitale (énergie, transports, santé, etc.) sont victimes chaque jour en France de plusieurs millions d'attaques informatiques.

Dans mon rapport, je mentionne trois exemples :

Premier exemple : la perturbation de sites institutionnels, à l'image du site Internet du Sénat, rendu inaccessible fin 2011 lors de la discussion de la loi sur le génocide arménien ; Il s'agit de ce que les spécialistes appellent une attaque par « déni de service » : le site Internet est rendu inaccessible car il est saturé de milliers de requêtes ;

Deuxième exemple : l'attaque informatique massive dont a fait l'objet, fin 2010, le ministère de l'économie et des finances, dans le cadre de la préparation de la présidence française du G8 et du G20 : il s'agit là d'une vaste intrusion informatique à des fins d'espionnage : un logiciel espion est introduit grâce à un « cheval de Troie », qui se présente sous la forme d'une pièce jointe piégée ouvrant une « porte dérobée » ; l'attaquant peut alors surveiller et prendre, à distance et à l'insu de l'utilisateur, le contrôle de son ordinateur, par exemple pour extraire des données, lire ses messages

électroniques, et même écouter ses conversations ou filmer sa victime en déclenchant lui-même le micro ou la caméra de l'ordinateur ; il peut ensuite, par rebonds successifs, prendre le contrôle d'autres ordinateurs, voire de la totalité du système ;

Troisième illustration : l'affaire d'espionnage, révélée par la presse, subie par le groupe AREVA : là aussi nous sommes face à une vaste intrusion informatique à des fins d'espionnage mais qui concerne cette fois une grande entreprise française du nucléaire.

Ces attaques peuvent être menées par des « pirates informatiques », des groupes d'activistes, des organisations criminelles, mais aussi par des entreprises concurrentes, voire par d'autres Etats. Les soupçons se portent souvent vers la Chine ou la Russie, même s'il est très difficile d'identifier précisément les auteurs de ces attaques. Ainsi, dans le cas de Bercy, comme d'AREVA, certains indices peuvent laisser penser que des agences officielles, ou du moins des officines chinoises, sont à l'origine de ces attaques.

Par ailleurs, les révélations du journaliste américain David Sanger sur l'implication des Etats-Unis dans la conception du virus STUXNET, qui a endommagé un millier de centrifugeuses d'enrichissement de l'uranium, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran, ou encore la récente découverte du virus FLAME, vingt fois plus puissant que STUXNET, laissent présager de futures « armes informatiques » aux potentialités encore largement ignorées.

La conclusion que je tire de tout cela est que nous voyons bien s'ouvrir, pour les années qui viennent, un nouveau champ de bataille, avec des stratégies et des effets très spécifiques.

On peut s'interroger sur la nature de cette menace. Peut-on parler de « cyberguerre » et imaginer que les conflits se joueront sur des « cyberattaques », qui se substitueraient aux modes d'action militaires traditionnels ? C'est sans doute une hypothèse assez extrême.

Il me semble acquis en revanche que l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information. C'est par exemple ce qui s'est passé en Géorgie en août 2008. Toutes les armées modernes ont commencé à intégrer ce facteur.

Jusqu'à présent, ce type d'attaques n'a généré que des nuisances assez limitées. Mais, à mon sens, il ne faut pas s'illusionner. Les vulnérabilités sont réelles et les savoir-faire se développent. On ne peut pas éviter de telles attaques. Mais on peut en limiter les effets en renforçant les mesures de protection et en prévoyant comment gérer la crise le temps du rétablissement des systèmes.

Lors de mes différents déplacements à l'étranger, j'ai été d'ailleurs frappé de voir que chez nos principaux alliés, la thématique de la cyberdéfense ne cesse de monter en puissance.

C’est le cas aux Etats-Unis. Le Président Barack Obama s’est fortement engagé sur le sujet et a qualifié la cybersécurité de priorité stratégique.

Comme j’ai pu le constater lors de mon déplacement à Washington, il existe plusieurs organismes, au sein du département chargé de la sécurité intérieure et du Pentagone qui interviennent dans ce domaine, comme la NSA ou le Cybercommand, et la coordination entre ces organismes n’est pas toujours optimale.

De 2010 à 2015, le gouvernement américain devrait cependant consacrer 50 milliards de dollars à la cyberdéfense et plusieurs dizaines de milliers d’agents travaillent sur ce sujet.

Au Royaume-Uni, le gouvernement britannique a adopté, en novembre dernier, une nouvelle stratégie en matière de sécurité des systèmes d’information.

Le principal organisme chargé de la cybersécurité est le « Government Communications Headquarters » (GCHQ). Environ 700 agents s’occupent des questions liées à la cyberdéfense.

Malgré la réduction des dépenses publiques, le Premier ministre David Cameron a annoncé en 2010 un effort supplémentaire de 650 millions de livres sur les quatre prochaines années pour la cyberdéfense, soit environ 750 millions d’euros. Ces chiffres peuvent laisser songeur lorsque l’on sait qu’en France le budget de l’agence homologue, l’ANSSI, est de 75 millions d’euros.

En Allemagne, le gouvernement fédéral a élaboré en février 2011 une stratégie en matière de cybersécurité.

La coordination incombe au ministère fédéral de l’Intérieur, auquel est rattaché l’office fédéral de sécurité des systèmes d’information (BSI), situé à Bonn, qui dispose d’un budget annuel de 80 millions d’euros et de plus de 500 agents.

Toujours sur ce volet international, les cyberattaques sont désormais une menace prise en compte dans le nouveau concept stratégique de l’Alliance atlantique, adopté lors du Sommet de Lisbonne en novembre 2010.

L’OTAN s’est dotée en juin 2011 d’une politique et d’un concept en matière de cyberdéfense. Une autorité de gestion de la cyberdéfense, ainsi qu’un centre d’excellence sur la cyberdéfense situé à Tallin en Estonie ont été créés.

Pour autant, l’OTAN n’est pas complètement armée face à cette menace.

Ainsi, la principale unité informatique de l’Alliance n’est toujours pas opérationnelle 24 heures sur 24, 7 jours sur 7 et elle n’assure pas encore la sécurité de tous les réseaux de l’OTAN.

D'ailleurs, l'OTAN a été la cible de plusieurs attaques informatiques l'été dernier, attaques attribuées à la mouvance Anonymous et même l'ordinateur personnel du Secrétaire général de l'OTAN a été « piraté ».

Plus généralement, l'OTAN doit encore déterminer quelle attitude adopter pour répondre à des cyberattaques lancées contre l'un des Etats membres. Peut-on invoquer l'article 5 du traité de Washington en cas de cyberattaque ? Les mesures de rétorsion doivent-elles se limiter à des moyens cybernétiques, ou bien peut-on également envisager des frappes militaires conventionnelles ?

Il n'y a pas encore de réponses claires à ces questions, comme j'ai pu le constater lors de mes entretiens au siège de l'OTAN.

L'Union européenne a aussi un grand rôle à jouer, car une grande partie des règles qui régissent les réseaux de communications électroniques relèvent de sa compétence.

Elle peut donc agir pour l'harmonisation de certaines dispositions techniques au niveau européen qui sont importantes du point de vue de la cyberdéfense.

Toutefois, la Commission européenne et de nombreux pays européens ne semblent pas encore avoir pris la mesure des risques et des enjeux liés à la cyberdéfense.

Ainsi, l'agence européenne chargée de la sécurité des réseaux et de l'information, ENISA, créée en 2004 et dont le siège est situé à Héraklion, en Crète, ne dispose que d'un rôle de recommandation et son efficacité apparaît assez limitée.

Ceci m'amène à évoquer la situation de la France.

Le constat que notre commission avait dressé dans son rapport il y a quatre ans était assez brutal : face à cette menace réelle et croissante, la France n'était ni bien préparée, ni bien organisée.

Il serait injuste de dire que rien n'avait été fait. Je pense au réseau gouvernemental ISIS pour l'information confidentiel défense.

Néanmoins, les lacunes restaient criantes. En d'autres termes, il paraissait absolument indispensable d'accélérer la prise de conscience des autorités politiques, de clarifier les responsabilités au sein de l'Etat et de renforcer résolument les moyens techniques et humains nécessaires à une vraie politique de cyberdéfense.

Le Livre blanc sur la défense et la sécurité nationale de 2008 a identifié ce besoin et donné une réelle impulsion à cette politique.

En termes d'organisation, le Livre blanc a permis à cette politique d'être clairement identifiée, avec la création, en juillet 2009, de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, qui est dirigée

par M. Patrick Pailloux, et dont les compétences sont reconnues par tous en France comme à l'étranger.

En février 2011, l'ANSSI a rendu publique la stratégie de la France en matière de cyberdéfense. Il a été également décidé de faire de l'ANSSI l'autorité nationale de défense des systèmes d'information.

La France dispose, avec cette stratégie et avec l'ANSSI, d'outils importants en matière de cyberdéfense. Pour autant, beaucoup reste à faire dans ce domaine.

Ainsi, avec des effectifs de 230 personnes et un budget de l'ordre de 75 millions d'euros, les effectifs et les moyens de l'ANSSI sont encore très loin de ceux dont disposent les services similaires de l'Allemagne ou du Royaume-Uni, qui comptent entre 500 et 700 personnes.

Pour accroître sa capacité d'intervention et de soutien, le gouvernement de François Fillon avait d'ailleurs décidé, en mai dernier, d'accélérer l'augmentation des effectifs et des moyens de l'ANSSI, afin de porter ses effectifs à 360 d'ici 2013.

De plus, si les armées et le ministère de la défense ont pris des mesures, les autres ministères, les entreprises et les opérateurs d'importance vitale restent différemment sensibilisés à cette menace.

Quel serait aujourd'hui le moyen le plus simple de provoquer une perturbation majeure de notre pays par le biais d'une attaque informatique ? Un moyen très simple serait de s'en prendre aux systèmes de distribution d'énergie, aux transports ou aux hôpitaux.

L'exemple du virus STUXNET, ou du ver Conficker qui a perturbé le fonctionnement de plusieurs hôpitaux en France et dans le monde, montrent que cela n'est pas une hypothèse d'école.

Il ne s'agit pas de prétendre à une protection absolue. Ce serait assez illusoire. Le propre des attaques informatiques est d'exploiter des failles, de se porter là où les parades n'ont pas encore été mises en place. Mais on peut renforcer la sécurité des réseaux et des infrastructures les plus sensibles, et améliorer leur résilience.

J'en viens aux 10 priorités proposées dans mon rapport.

Premièrement, il me semble que la protection et la défense des systèmes d'information devrait faire l'objet d'une véritable priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire.

Il me paraît ainsi indispensable de renforcer les effectifs et les moyens de l'ANSSI au moyen d'un plan pluriannuel, afin de les porter progressivement à la hauteur de ceux dont disposent nos principaux partenaires européens.

Cette augmentation, de l'ordre de quelques 80 agents par an, devrait au demeurant rester modeste.

Deuxièmement, il me semble que beaucoup reste à faire pour sensibiliser les administrations, le monde de l'entreprise, notamment les PME, et les opérateurs d'importance vitale.

Assurer la sécurité des systèmes d'information des entreprises n'est pas seulement un enjeu technique. C'est aussi un enjeu économique, puisqu'il s'agit de protéger la chaîne de valeur, notre savoir-faire technologique dans la véritable guerre économique que nous connaissons aujourd'hui, voire un enjeu politique, lorsque les intérêts de la nation sont en jeu.

Or, avec l'espionnage informatique, notre pays, comme les autres pays occidentaux, est aujourd'hui menacé par un « pillage » systématique de son patrimoine diplomatique, culturel et économique.

L'ANSSI s'efforce d'inciter les entreprises à respecter des règles élémentaires de sécurité, règles que son directeur général, M. Patrick Pailloux, assimile à des règles d'hygiène numérique élémentaires, mais qui sont souvent considérées comme autant de contraintes par les utilisateurs.

Faut-il aller plus loin et passer par la loi pour fixer un certain nombre de règles ou de principes ?

Après avoir beaucoup consulté, je crois qu'il est nécessaire de prévoir une obligation de déclaration en cas d'attaques informatiques qui s'appliquerait aux entreprises et aux opérateurs des infrastructures vitales, afin que l'Etat puisse être réellement informé de telles attaques.

Je pense aussi que l'Etat a un rôle important à jouer pour soutenir le tissu industriel, et notamment les PME, qui développent en France des produits ou des services de sécurité informatique, pour ne pas dépendre uniquement de produits américains ou asiatiques.

Je plaide ainsi dans mon rapport pour une politique industrielle volontariste, à l'échelle nationale et européenne, pour faire émerger de véritables « champions » nationaux ou européens.

A cet égard, j'insiste dans mon rapport sur la question des « routeurs de cœur de réseaux », sujet qui a été évoqué très souvent par mes différents interlocuteurs, français ou étrangers.

Ces « routeurs » sont de grands équipements informatiques utilisés par les opérateurs de télécommunications pour gérer les flux de communications (comme les messages électroniques ou les conversations téléphoniques) qui transitent par l'Internet.

Ils représentent des équipements hautement sensibles car ils ont la capacité d'intercepter, d'analyser, d'exfiltrer, de modifier ou de détruire toutes les informations qui passent par eux.

Actuellement, le marché des routeurs est dominé par des entreprises américaines, comme Cisco, mais, depuis quelques années, des entreprises chinoises, à l'image de Huawei et ZTE, font preuve d'une forte volonté de pénétration sur le marché mondial et en Europe.

Cette stratégie est d'ailleurs encouragée par certains opérateurs de télécommunications, car les routeurs chinois sont environ 20 % moins chers que les routeurs américains ou européens.

Or, comme cela m'a été confirmé à plusieurs reprises lors de mes entretiens, cette stratégie soulève de fortes préoccupations, en raison des liens de ces entreprises avec le gouvernement chinois et des soupçons d'espionnage informatique qui pèsent sur la Chine.

Ainsi, les autorités américaines, comme d'ailleurs les autorités australiennes, ont refusé l'utilisation de « routeurs » chinois sur leur territoire pour des raisons liées à la sécurité nationale.

En Europe, une telle interdiction semble plus délicate mais la Commission européenne s'apprêterait à lancer une procédure d'infraction à l'encontre de ces entreprises, soupçonnées de concurrence déloyale.

Pour ma part, je considère qu'il est indispensable que l'Union européenne, à l'image des Etats-Unis ou de l'Australie, interdise l'utilisation des « routeurs » ou autres équipements informatiques sensibles d'origine chinoise sur son territoire. Il s'agit là d'un véritable enjeu de sécurité nationale.

Se pose également la question des ressources humaines. Il existe aujourd'hui peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à en recruter.

Nous devrions mettre l'accent sur la formation et développer les liens avec les universités et les centres de recherche.

A cet égard, pourquoi ne pas renforcer aussi les liens avec la « communauté de hackers » français, dont la plupart sont désireux de mettre leurs compétences et leurs talents au service de leur pays ?

Il paraît également nécessaire de renforcer la sensibilisation des utilisateurs.

De même qu'il existe un plan de prévention en matière de sécurité routière, pourquoi ne pas imaginer une campagne de communication en matière de sécurité informatique ?

Face à une menace qui s'affranchit des frontières, la coopération internationale sera déterminante.

Elle existe d'ores et déjà entre les cellules gouvernementales spécialisées ou de manière bilatérale, notamment avec nos partenaires britanniques ou allemands.

Elle arrive à l'ordre du jour d'enceintes internationales comme l'OTAN ou l'Union européenne, qui pourrait s'impliquer plus activement, par exemple pour imposer un certain nombre de normes de sécurité aux opérateurs de réseaux.

Pour autant, si la coopération internationale est indispensable, notamment avec nos partenaires britanniques et allemands, il ne faut pas se faire trop d'illusions.

La cyberdéfense est une question qui touche à la souveraineté nationale et il n'existe pas réellement d'alliés dans le cyberespace.

Enfin, je pense qu'il faut nous poser la question délicate des capacités offensives.

Il existe sur ce sujet en France un véritable « tabou », comme j'ai pu moi-même le constater lors de mes différents entretiens.

A l'inverse, d'autres pays, comme les Etats-Unis ou le Japon, n'hésitent pas à affirmer qu'ils répondront à une attaque informatique.

Pour ma part, je pense qu'on ne peut pas se défendre si l'on ne connaît pas les modes d'attaque.

La lutte informatique offensive est prévue par le Livre blanc et la loi de programmation militaire.

Mais toutes ses implications ne sont pas aujourd'hui clarifiées.

Comment savoir si une attaque se prépare ou est en cours ? Comment établir l'identité des agresseurs ou la responsabilité d'un Etat ? Quelle doctrine d'emploi adopter ? Il faudra que nos experts trouvent des réponses à ces questions.

Dans mon rapport, je m'interroge donc sur l'opportunité de définir une doctrine publique sur les capacités offensives, qui pourrait être reprise par le nouveau Livre blanc sur la défense et la sécurité nationale.

Je ne sais pas si l'on verra à l'avenir des cyberguerres. Mais je suis certain que notre défense et notre sécurité se joueront aussi sur les réseaux informatiques et au sein de nos systèmes d'information dans les années futures.

Je vous remercie de votre attention et je suis disposé à répondre à vos questions.

A la suite de cette présentation, un débat s'est engagé au sein de la commission.

M. Jean-Louis Carrère, président – Je vous remercie pour votre excellent rapport qui marque la conclusion des travaux de notre commission consacrés à la préparation de la révision du Livre blanc sur la défense et la sécurité nationale. Je laisse tout de suite la parole à nos collègues qui auront certainement beaucoup de questions à vous poser.

Mme Nathalie Goulet. – Vous avez insisté dans votre présentation sur l'importance de la formation d'ingénieurs spécialisés et les difficultés rencontrées par les entreprises ou les administrations pour en recruter, et je m'en félicite.

Je souhaiterais vous interroger au sujet du rôle des hauts fonctionnaires de défense et de sécurité qui sont présents au sein de chaque ministère et de leurs relations avec l'ANSSI et le SGDSN. J'ai pu constater, en effet, que la mission de ces hauts fonctionnaires de défense et de sécurité et leur coordination n'étaient pas toujours optimales et je pense qu'il serait utile d'avoir une réflexion concernant le rôle des hauts fonctionnaires de défense et de sécurité au sein de chaque ministère.

Par ailleurs, je m'interroge au sujet de l'organisation institutionnelle en matière de protection et de défense des systèmes d'information et notamment de la coordination interministérielle dans ce domaine. Le modèle actuel vous semble-t-il pertinent et la coordination interministérielle fonctionne-t-elle de manière satisfaisante, notamment entre l'ANSSI et le ministère de la défense ? Cette coordination doit-elle d'après vous relever du Président de la République, du Premier ministre, du SGDSN ou bien être rattachée au ministère de la défense ?

M. Yves Pozzo di Borgo. – Je partage également votre sentiment concernant l'importance de la formation d'ingénieurs spécialisés dans la sécurité des systèmes d'information. Comment, d'après vous, inciter les étudiants à suivre ce type de formation et comment inciter les écoles d'ingénieurs ou d'informatique à former davantage de spécialistes dans ce domaine ?

Il me semble aussi que la recherche n'est pas suffisamment développée en France et que nous manquons de laboratoires ou de centres de recherche dans certains domaines clés pour la sécurité des systèmes d'information, notamment par rapport à ce qui existe aux Etats-Unis. Quelles sont vos préconisations concernant le renforcement de la recherche dans ces domaines ?

Par ailleurs, vous avez mentionné la communauté de « hackers » en soulignant qu'il serait utile de renforcer les liens avec cette communauté étant donné que la plupart de ces « hackers » disposent de très grandes compétences dans ces domaines et que la plupart d'entre eux seraient désireux de mettre leurs talents au service de notre pays. Mais s'agit-il pour les services de l'Etat de recruter des « hackers » ? Comment concrètement renforcer les liens avec cette communauté ?

Enfin, quelles sont les raisons pour lesquelles il est très difficile d'identifier précisément les auteurs des attaques contre les systèmes d'information ? Est-ce que cela résulte de difficultés techniques ou bien plutôt d'une coopération internationale insuffisante ? Il semblerait que les attaques informatiques importantes ne soient plus, comme auparavant, le fait de pirates

informatiques individuels, particulièrement doués, mais de véritables organisations, voire de services étatiques.

M. Didier Boulaud. – Je considère qu'il est très important que notre commission suive avec une grande attention les questions relatives à la protection et à la défense des systèmes d'information et je pense que ce rapport, qui intervient après l'excellent rapport de notre ancien collègue M. Roger Romani, permettra de renforcer la sensibilisation de l'ensemble des acteurs mais aussi de l'opinion à l'importance des enjeux.

Concernant toutefois les "capacités offensives", je m'en tiendrai, pour ma part, à la plus grande prudence et j'appliquerai le proverbe selon lequel « moins on en parle, mieux on se porte ».

Je suis donc réservé sur votre proposition concernant l'élaboration d'une doctrine publique sur les capacités offensives.

Comment, en effet, reconnaître publiquement que l'on développe des « capacités offensives », alors que toute intrusion dans les systèmes d'information est illégale au regard de notre législation ?

M. Jean-Marie Bockel, rapporteur. – Je vous remercie pour vos observations.

Il existe certes au sein de chaque ministère un haut fonctionnaire de défense et de sécurité (HFDS), mais cette fonction est souvent cumulée par le secrétaire général du ministère concerné, ce qui ne lui permet pas de se consacrer entièrement à cette tâche. Il existe aussi au sein de chaque ministère un fonctionnaire de la sécurité des systèmes d'information (FSSI). Mais on constate que celui-ci n'occupe souvent qu'une faible place hiérarchique au sein de l'organigramme et surtout qu'il ne parvient pas à imposer aux différentes directions sectorielles et aux directeurs des systèmes d'information une prise en compte suffisante des préoccupations liées à la sécurité des systèmes d'information. C'est la raison pour laquelle je propose, dans mon rapport, de rehausser le statut des fonctionnaires de la sécurité des systèmes d'information et de renforcer leurs prérogatives par rapport aux responsables des différentes directions. Les fonctionnaires de la sécurité des systèmes d'information devraient, à mes yeux, devenir de véritables directeurs, voire même des secrétaires généraux, chargés de la sécurité et de la défense des systèmes d'information au sein de chaque ministère. Ainsi, pour prendre l'exemple du ministère de la défense, je propose de rehausser le statut du fonctionnaire de la sécurité des systèmes d'information, afin que celui-ci dispose en particulier d'une réelle autorité sur la sous-direction et les équipes chargées de la sécurité des systèmes d'information au sein de la direction générale des systèmes d'information et de communication (DGSIC).

Ayant pu comparer le dispositif français avec les différents modèles étrangers, notamment aux Etats-Unis, au Royaume-Uni et en Allemagne, je considère que l'organisation institutionnelle française en matière de protection et de défense des systèmes d'information est la plus pertinente car elle

correspond le mieux à l'organisation administrative et à la culture de notre pays.

Notre modèle se caractérise, en effet, par son caractère centralisé et interministériel, puisque l'agence nationale de la sécurité des systèmes d'information est une agence rattachée au Secrétaire général de la défense et de la sécurité nationale, ce qui lui confère une légitimité interministérielle vis-à-vis des autres ministères. Le ministère de la défense et les armées, comme d'autres ministères, ont certes un rôle spécifique à jouer, mais, comme j'ai pu moi-même le constater, les relations entre l'ANSSI et le ministère de la défense sont excellentes, comme en témoigne la coopération étroite entre le directeur général de l'ANSSI, M. Patrick Pailloux, et l'officier général cyberdéfense à l'état-major des armées, le Contre-amiral Arnaud Coustillière, dont les compétences sont unanimement appréciées.

Je considère aussi que le rattachement de l'ANSSI au Secrétaire général de la défense et de la sécurité nationale, qui dépend du Premier ministre, est une bonne chose.

La coordination ne peut relever, d'après moi, que de l'autorité du Premier ministre, à qui il appartient de définir les axes stratégiques, de suivre leur mise en œuvre et de veiller à la bonne répartition des moyens humains, techniques et financiers.

Notre modèle se caractérise également par une stricte séparation entre les aspects préventifs et défensifs, confiés à l'ANSSI, et les aspects offensifs, qui relèvent des armées et des services spécialisés, ce qui me paraît également préférable, étant donné la nécessité d'établir des liens étroits entre l'ANSSI et le secteur privé.

Comme le souligne très bien notre collègue M. Yves Pozzo di Borgo, il existe en France peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises, ainsi que les administrations, ont du mal à en recruter.

Il semblerait qu'il y ait quatre à cinq fois plus d'offres d'emplois disponibles, dans les administrations ou les entreprises, que d'ingénieurs spécialement formés à la sécurité informatique sortant des écoles d'ingénieurs.

Je considère donc qu'il serait souhaitable d'encourager les écoles d'ingénieurs à développer les formations en matière de sécurité des systèmes d'information. Plus généralement, la protection des systèmes d'information devrait être une étape obligée dans le cursus de l'ensemble des formations d'ingénieur ou d'informatique et il me semblerait utile d'inclure une sensibilisation obligatoire dans les écoles formant les cadres de l'administration, comme l'ENA par exemple, et de proposer une telle sensibilisation aux formations de management destinée aux entreprises.

Une autre priorité concerne effectivement la recherche.

Si notre pays dispose de centres d'excellences reconnus dans certains domaines clés pour la défense et la sécurité des systèmes d'information, comme celui de la cryptologie ou des cartes à puces, de manière générale, la recherche semble insuffisamment développée en France, notamment par rapport à ce qui existe aux Etats-Unis.

Ainsi, notre pays manque ainsi cruellement de laboratoires travaillant sur des sujets clés, essentiels à une réelle maîtrise des enjeux nationaux en termes de sécurité des systèmes d'information.

Par ailleurs, notre pays souffre d'un manque de stratégie commune et de l'éparpillement des différents organismes publics de recherche (CNRS, INRIA, CEA-LETI), qui s'ignorent le plus souvent, et d'une coopération insuffisante de ces organismes avec l'ANSSI et la DGA.

Dans mon rapport, je suggère plusieurs pistes d'amélioration, comme la création d'un budget spécifique de recherche et développement dans ce secteur, la mise en place d'un comité mixte à l'image de ce qui a été fait dans le domaine du nucléaire, ou du moins d'un comité stratégique afin de rapprocher les différents acteurs publics. Par ailleurs, afin de renforcer la recherche et de rapprocher les différents acteurs publics mais aussi l'Etat, les entreprises, les universités et les centres de recherches, la création d'une fondation est actuellement à l'étude et me paraît devoir être encouragée.

Concernant le renforcement des liens avec la communauté de « hackers », il ne s'agit pas, dans mon esprit, de recourir à des « pirates informatiques » pour lancer des attaques. Mais on pourrait reconnaître et encourager davantage l'activité des sociétés privées de conseil en sécurité informatique, de manière encadrée, par un système d'agrément ou de label, et envisager des modifications législatives, par exemple concernant la communication ou la publication des failles ou vulnérabilités des systèmes d'information à des fins de conseil ou de recherche.

Enfin, il est très difficile d'identifier précisément le commanditaire d'une attaque informatique car les pirates informatiques ont très souvent recours à des « botnets », c'est-à-dire à des réseaux de machines compromises (ou machines « zombies »), situées partout dans le monde.

Le « botnet » est constitué de machines infectées par un virus informatique contracté lors de la navigation sur internet, lors de la lecture d'un courrier électronique (notamment les spams) ou lors du téléchargement de logiciels. Ce virus a pour effet de placer la machine, à l'insu de son propriétaire, aux ordres de l'individu ou du groupe situé à la tête du réseau. On estime aujourd'hui que le nombre de machines infectées passées sous le contrôle de pirates informatiques est considérable. Le détenteur du réseau est rarement le commanditaire de l'attaque. Il monnaye sa capacité d'envoi massive à des « clients » animés de préoccupations diverses.

Enfin, concernant les « capacités offensives », je comprends les réserves de notre collègue M. Didier Boulaud. Certes, il ne faut pas négliger

les inconvénients pour notre pays qu'il y aurait à évoquer publiquement ce sujet, qui tiennent essentiellement à la crainte de donner une sorte de légitimité aux attaques informatiques d'origine étatique et d'encourager ainsi les autres pays à développer et à utiliser de telles capacités, ainsi que le risque de dévoiler aux yeux de tous l'étendue de notre expertise dans ce domaine, ce qui pourrait conduire à affaiblir la portée de ces capacités.

Il ne paraît pas évident en effet pour un Etat de reconnaître publiquement vouloir se doter d'« armes informatiques », étant donné que toute intrusion dans un système informatique est généralement condamnée par la loi.

On le voit bien avec la polémique suscitée par les révélations du journaliste américain David Sanger sur l'implication des Etats-Unis dans la conception du virus STUXNET.

Toutefois, je voudrais rappeler que les « capacités offensives » étaient déjà évoquées dans le Livre blanc sur la défense et la sécurité nationale de 2008.

Le silence absolu des autorités françaises sur cette question depuis le Livre blanc de 2008 paraît donc quelque peu en décalage avec l'évolution de la menace, les communications publiques de nos principaux partenaires, et il pourrait même être de nature à entretenir des fantasmes dans l'opinion publique.

Surtout, le développement de « capacités offensives » nécessite une anticipation opérationnelle, une préparation technique et un travail très important, portant non seulement sur l'arme informatique elle-même, mais aussi sur le recueil de renseignement, la désignation de cibles potentielles, l'analyse des systèmes d'information ainsi que leur environnement, l'identification des vulnérabilités, avec la nécessité de procéder à des entraînements en liaison étroite avec d'autres modes d'interventions (armes conventionnelles, missiles balistiques, etc.) ou encore un travail sur la définition même d'une « arme informatique » et les conditions de son emploi dans le cadre du droit des conflits armés.

Il me semble donc qu'il serait souhaitable que les autorités françaises lancent une réflexion sur l'élaboration d'une éventuelle doctrine ou du moins d'un discours ayant vocation à être rendu publics sur les « capacités offensives », notamment dans le cadre du nouveau Livre blanc sur la défense et la sécurité nationale.

M. Robert del Picchia. – Je partage votre sentiment concernant l'utilité de renforcer les liens avec la communauté de « hackers ». Mais, est-ce que les services de l'Etat, comme l'ANSSI ou d'autres services, recrutent des « hackers » ?

M. Jean-Marie Bockel, rapporteur. – Il existe plusieurs catégories de « hackers ». On distingue, en effet, les « chapeaux blancs » (« white hats »), qui sont les administrateurs ou les cyberpoliciers, qui recherchent les

logiciels malveillants et qui se caractérisent par leur sens de l'éthique et de la déontologie. Les « chapeaux gris » (« grey hats ») pénètrent dans les systèmes sans y être autorisés, pour faire la preuve de leur habileté ou pour alerter l'organisme visé des vulnérabilités de ses systèmes, mais ils ne sont pas animés par des intentions malveillantes ou criminelles. Enfin, les « chapeaux noirs » (« black hats ») regroupent les « cybercriminels », les « cyberespions » ou les « cyberterroristes ». Ce sont eux qui répandent volontairement les virus informatiques. Ils sont essentiellement motivés par l'appât du gain. Ces individus ou ces groupes mettent au point des outils qu'ils peuvent exploiter directement ou offrir sur le marché à des clients tels que des organisations criminelles ou mafieuses, des officines d'espionnage économique, des entreprises ou encore des services de renseignement.

M. Robert del Picchia. – Vous avez mentionné les risques qui pèsent sur la sécurité informatique des entreprises ou des opérateurs d'importance vitale et je partage vos préoccupations. Je suis notamment préoccupé par le risque de divulgation des données personnelles. Sommes-nous réellement à l'abri d'un risque de pénétration dans les systèmes d'information d'un organisme comme la CNIL par exemple ? Un autre risque majeur tient aux opérateurs d'importance vitale. Il y a quelques jours, le réseau de l'opérateur Orange a été fortement perturbé en France pendant plusieurs heures à la suite, semble-t-il, d'une panne informatique. Mais, comment ne pas imaginer les effets catastrophiques d'une attaque informatique massive contre les opérateurs de télécommunications, le système bancaire, les réseaux de transport ou encore la distribution d'énergie ?

Enfin, qu'en est-il des entreprises françaises spécialisées dans la conception de produits ou l'offre de services en matière de sécurité informatique ?

M. Daniel Reiner. – Je vous remercie également pour votre rapport très intéressant et je me félicite que notre commission ait jugé utile de se pencher à nouveau sur ce sujet, qui présente une grande importance pour notre défense et notre sécurité. Ce rapport intervient également au bon moment et j'espère qu'il sera pris en compte, comme les précédents rapports de notre commission, dans le cadre des réflexions de la commission chargée de la préparation du nouveau Livre blanc sur la défense et la sécurité nationale.

Je voudrais faire deux observations.

La première observation concerne les relations entre l'Etat et les entreprises. Dans le cadre de l'assemblée parlementaire de l'OTAN, nous avions assisté, lors d'une réunion à Bruxelles, en février dernier, à une présentation très intéressante d'un représentant de Microsoft, qui nous avait expliqué que son entreprise faisait l'objet d'un grand nombre d'attaques informatiques et qu'elle consacrait des moyens financiers très élevés au renforcement de la sécurité de ses propres produits informatiques. Ne serait-il pas utile de préconiser, non seulement un renforcement des relations, mais une véritable coopération entre le secteur public et le secteur privé en matière de

protection et de défense des systèmes d'information ? Je pense que vous pourriez insister sur ce point dans vos recommandations.

Ma deuxième observation porte sur les « routeurs de cœur de réseaux ». Vous préconisez, dans votre rapport, d'interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de « routeurs » ou d'autres équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les « routeurs » et certains équipements d'origine chinoise.

Pour ma part, je ne vois pas l'utilité de ce deuxième membre de phrase et je serai plutôt favorable à l'idée de le supprimer, car dès lors qu'un équipement présente un risque pour la sécurité nationale, quelle que soit son origine, son utilisation devrait être interdite sur notre territoire.

Comme vous le savez certainement, les autorités américaines procèdent actuellement à une vaste expertise de leurs équipements et réseaux informatiques, car ils ont découvert récemment que ces équipements et systèmes, y compris les plus sensibles, comprenaient de nombreux composants informatiques d'origine chinoise dont ils ne soupçonnaient pas l'existence et dont ils voudraient être certains qu'ils présentent toutes les garanties en matière de sécurité informatique. Ne serait-il pas utile de préconiser de lancer une telle expertise aussi dans notre pays ?

Mme Joëlle Garriaud-Maylam. – Je voudrais remercier notre rapporteur pour la qualité de son rapport. Je partage en particulier l'idée de promouvoir une plus grande sensibilisation des utilisateurs, qui me paraît très importante, et je souscris à votre idée d'une campagne d'information inspirée de la prévention routière. Je pense, en effet, que beaucoup reste à faire en matière de sensibilisation des utilisateurs, notamment face aux risques soulevés par la cybercriminalité, comme l'illustrent les nombreuses tentatives d'escroquerie par Internet, que nous recevons chaque jour sur notre messagerie.

A cet égard, que pensez vous du portail Internet consacré à la sécurité informatique : http://www.securite-informatique.gouv.fr/ ? Est-ce un instrument réellement utile en matière de sensibilisation du grand public ?

M. Jeanny Lorgeoux. – Qu'en est-il exactement de la coopération avec nos partenaires européens dans ce domaine et quel est votre sentiment au sujet de l'organisation et des moyens mis en place aux Etats-Unis ?

M. Jean-Marie Bockel, rapporteur. – Je partage entièrement l'analyse de notre collègue M. Daniel Reiner, concernant la nécessité d'un renforcement de la coopération entre l'Etat et le secteur privé. J'accepte donc volontiers de modifier la rédaction de mon rapport sur ce point.

Concernant les « routeurs de cœur de réseaux », je rappelle qu'il s'agit de grands équipements d'interconnexion de réseaux informatiques utilisés par les opérateurs de télécommunications qui permettent d'assurer le

flux des paquets de données entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

La fiabilité de ces « routeurs » doit être à toute épreuve, leur sécurisation renforcée et leur surveillance assurée car toute perturbation du « routeur » peut isoler un site du reste du monde ou engendrer une compromission de l'intégralité des données transitant par cet équipement.

De plus, rien n'empêcherait un pays producteur de ce type d'équipements d'y placer un dispositif de surveillance, d'interception, voire un système permettant d'interrompre à tout moment l'ensemble des flux de communication.

Le fait de placer un tel dispositif de surveillance directement au cœur du « routeur de réseaux » rendrait ce dispositif presque totalement « invisible » et indétectable. Et il n'est pas indifférent de savoir que de forts soupçons pèsent sur la Chine en matière de provenance des attaques informatiques, notamment à des fins d'espionnage économique.

Aux Etats-Unis, les autorités ont d'ailleurs pris ces dernières années plusieurs mesures afin de limiter la pénétration des équipementiers chinois Huawei et ZTE sur le marché américain pour des raisons liées à la sécurité nationale.

Les autorités américaines soupçonnent que les puces, routeurs et autres équipements informatiques chinois soient équipés de « portes dérobées » permettant au gouvernement chinois d'accéder à des informations sensibles transitant par ces équipements. Les autorités australiennes ont également interdit l'utilisation des « routeurs » d'origine chinoise sur leur territoire, pour des raisons liées à la sécurité nationale.

Ces soupçons semblent d'ailleurs avoir été confirmés récemment, de manière involontaire, par les représentants de l'entreprise chinoise Huawei eux-mêmes, lors d'une présentation devant une conférence organisée à Dubaï en février dernier.

En effet, dans leur présentation, ils auraient indiqué que, pour mieux assurer la sécurisation des flux de ses clients, Huawei « analysait » (grâce aux techniques dites de « deep packet inspection » ou DPI), l'ensemble des flux de communications (courriers électroniques, conversations téléphoniques, etc.) qui transitaient par ses équipements.

Si les représentants de l'entreprise voulaient démontrer avant tout les capacités de leurs « routeurs » en matière de détection de « logiciels malveillants », ils ont ainsi confirmé, comme cela a d'ailleurs été relevé par plusieurs participants à cette conférence, les capacités potentielles de ces « routeurs » à analyser, intercepter et extraire des données sensibles, voire à les altérer ou les détruire.

Il est donc crucial que l'Union européenne adopte une position ferme d'une totale interdiction concernant le déploiement et l'utilisation des

« routeurs » chinois sur le territoire européen, ou d'autres grands équipements informatiques d'origine chinoise ne présentant pas toutes les garanties en matière de sécurité informatique.

Je préconise aussi, dans mon rapport, de lancer une coopération industrielle entre la France et l'Allemagne ou à l'échelle européenne pour développer des « routeurs de cœur de réseaux » ou d'autres grands équipements informatiques européens, afin de ne plus dépendre uniquement de produits américains ou asiatiques.

En réponse à notre collègue M. Robert del Picchia, je voudrais souligner que j'insiste dans mon rapport sur l'importance d'assurer la protection des opérateurs d'importance vitale. Il s'agit, à mes yeux, d'un véritable enjeu de sécurité nationale. Or, dans ce domaine, notre pays a pris un certain retard, notamment par rapport à nos principaux alliés. Je propose ainsi de prévoir une obligation de déclaration d'incident pour les entreprises et les opérateurs d'importance vitale, afin que l'Etat puisse être réellement informé en cas d'attaque informatique importante. Concernant les systèmes d'information de l'Etat, je crois utile d'insister sur la mise en place du réseau interministériel de l'Etat (RIE), qui devrait regrouper l'ensemble des réseaux des ministères et qui permettra de réduire le nombre de passerelles d'interconnexion à l'Internet, et dont le déploiement devrait commencer en 2013.

Enfin, je plaide dans mon rapport pour une politique industrielle volontariste de l'Etat afin de soutenir le tissu des entreprises, notamment des PME, qui proposent des produits ou des services en matière de sécurité informatique et l'établissement d'un réseau de confiance entre l'Etat et ces entreprises.

Comme notre collègue Mme Joëlle Garriaud Maylam, je considère qu'il importe de renforcer les mesures de sensibilisation à destination des acteurs, comme du grand public.

L'ANSSI a certes développé une politique de communication, avec, par un exemple un portail Internet consacré à la sécurité informatique, un petit guide de sécurité informatique destiné aux collaborateurs des cabinets ministériels ou encore un guide sur la sécurité informatique des systèmes industriels. Mais, ces mesures restent très insuffisantes.

Si la compétence et l'efficacité de l'Agence nationale de sécurité des systèmes d'information sont unanimement reconnues, en France comme à l'étranger, comme j'ai pu le constater lors de mes différents déplacements, en revanche, sa notoriété est notoirement insuffisante et sa politique de communication est largement inaudible.

Ainsi, n'est-il pas paradoxal que le portail de la sécurité informatique ou le site Internet de l'agence française de sécurité des systèmes d'information soient aussi ternes et peu attractifs pour les internautes, avec notamment l'absence de tout moteur de recherche et des mises à jour aléatoires ?

Les informaticiens de l'agence sont pourtant réputés être les meilleurs de leur spécialité. Il devrait être relativement simple de rendre le site Internet de l'ANSSI et le portail plus attractifs et plus dynamiques, à l'image de ce qui existe d'ailleurs chez la plupart de nos partenaires étrangers.

De même, on peut regretter l'absence de toute politique de communication de l'agence dirigée spécialement vers les PME, alors même qu'elles sont les plus vulnérables aux attaques informatiques.

L'Agence pourrait, en liaison avec le ministère délégué chargé des PME, de l'innovation et de l'économie numérique, travailler avec les chambres de commerce et d'industrie, relais traditionnels vers les PME.

L'Agence devrait donc améliorer sa politique de communication – qu'il s'agisse des responsables politiques, des administrations, des entreprises ou du grand public. Ainsi, pourquoi ne pas diffuser plus largement la synthèse d'actualité de l'ANSSI sur les incidents informatiques, qui est actuellement envoyée à un nombre très restreint de personnes ?

Les mesures de sensibilisation des utilisateurs mériteraient également d'être fortement accentuées. Cela passe notamment par l'établissement de chartes à l'usage des utilisateurs au sein des entreprises comme des administrations, par un développement de la communication et de la formation. Ainsi, il semblerait utile de développer le programme de formation de l'ANSSI et de l'élargir à d'autres publics, notamment issu du secteur privé.

La politique de sensibilisation à destination du grand public ne doit pas non plus être négligée. De même qu'il existe un plan national de prévention en matière de sécurité routière, pourquoi ne pas imaginer également un plan de communication en matière de sécurité des systèmes d'information ?

Enfin, il faudrait qu'à l'image de ce qui existe aux Etats-Unis ou au Royaume-Uni, les responsables politiques de notre pays, y compris au plus haut niveau de l'Etat, se saisissent des enjeux liés à la sécurité des systèmes d'information afin que ces questions soient portées publiquement et qu'elles ne soient plus réservées uniquement à un petit cercle de spécialistes.

Pour répondre à notre collègue M. Jeanny Lorgeoux, il existe de nombreux organismes aux Etats-Unis, au sein du Pentagone ou du département chargé de la sécurité nationale, qui interviennent dans ce domaine, comme l'Agence de sécurité nationale (NSA) ou encore le Cybercommand, inauguré en 2010 et qui est chargé plus particulièrement de protéger les réseaux militaires américains, et la coordination n'est pas toujours optimale entre ces différentes entités. De 2010 à 2015, le gouvernement américain devrait consacrer 50 milliards de dollars à la cyberdéfense et plusieurs dizaines de milliers d'agents travaillent sur ce sujet.

Si, face à une menace qui s'affranchit des frontières, la coopération internationale est une nécessité, cette coopération se heurte toutefois en pratique à de nombreux obstacles.

Un premier frein tient au manque de confiance qui existe au niveau international. Etant donné la difficulté d'identifier précisément l'origine des attaques informatiques et les soupçons qui pèsent sur l'implication de certains Etats, la plupart des pays sont réticents à partager des informations ou des connaissances.

Une seconde limite s'explique par les préoccupations partagées par la plupart des Etats de préserver leur souveraineté nationale. Cela est particulièrement vrai concernant la conception des produits de sécurité informatique, notamment ceux destinés à protéger l'information de souveraineté.

Ainsi, on constate que de nombreux Etats privilégient les coopérations bilatérales avec leurs proches alliés et hésitent à évoquer ces sujets dans un cadre multilatéral.

Pour sa part, notre pays a une coopération très étroite avec nos partenaires britanniques et allemands. L'ANSSI a également signé un accord de coopération avec l'agence estonienne. La coopération avec les Etats-Unis existe, même si celle-ci est plus difficile, notamment en raison du très grand nombre d'organismes qui interviennent dans ce domaine et de la forte disproportion de moyens.

La commission adopte le rapport d'information à l'unanimité.

ANNEXE I -

LISTE DES PERSONNES AUDITIONNÉES

● Présidence de la République

Général Benoît PUGA, Chef d'état-major particulier du Président de la République

● Premier ministre

● Secrétariat général de la défense et de la sécurité nationale (SGDSN)

M. Francis DELON, Secrétaire général de la défense et de la sécurité nationale

● Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Patrick PAILLOUX, Directeur général

M. Christian DAVIOT, Chargé de mission Stratégie à l'ANSSI

● Secrétariat général du gouvernement (SGG)

M. Jérôme FILIPPINI, Directeur de la direction interministérielle des systèmes d'information et de communication de l'Etat (DISIC) et Mme Hélène BRISSET, directrice du programme Réseau Interministériel de l'Etat (RIE)

● Ministère de la défense

Contre-amiral Arnaud COUSTILLIÈRE, Officier général cyberdéfense à l'état-major des armées

Amiral Christian PÉNILLARD, directeur général des systèmes d'information et de communication

M. Guillaume POUPARD, chef du pôle sécurité des systèmes d'information à la Direction générale de l'armement

M. Christian PROTAR, Contrôleur des armées

● Ministère des Affaires étrangères et européennes

M. Jean-François BLAREL, Secrétaire général adjoint

M. Thomas BONDIGUEL, direction des affaires stratégiques

● Ministère de l'économie et des finances

M. Dominique LAMIOT, Secrétaire général

M. Jean-Pierre DARDAYROL, Ingénieur général des mines, membre du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET)

Mme Claudine DUCHESNE, Contrôleur général économique et financier, membre du CGEIET

● Ministère de l'intérieur

M. Stéphane TIJARDOVIC, Sous-directeur, direction générale de la police nationale

● Entreprises

- AREVA :

M. Bernard CARDEBAT, Responsable de la sécurité des systèmes d'information

M. Ahmed BENNOUR, Directeur des systèmes d'information

- EADS Cassidian

M. Hervé GUILLOU, Président directeur général

M. Sébastien HEON, directeur des relations institutionnelles du Cyber Center

M. Bénédicte SUZAN, Senior Analyst

- CEIS :

M. Guillaume TISSIER, directeur général

M. Rémi PAUTRAT, ancien Préfet

- SOGETI :

M. Luc-François SALVADOR, Président-directeur général

- SYSDREAM :

M. Olivier FRANCHI, Directeur associé

M. Guillaume VASSAULT-HOULIERE, Directeur technique et opérationnel

- THALES :

Mme Pascale SOURISSE, Président-directeur général de Thales communications et technologies

M. Stanislas de MAUPEOU, responsable cyberdéfense

Mme Isabelle CAPUTO, Directeur des relations parlementaires et politiques

● Experts

M. Nicolas ARPAGIAN, Directeur scientifique du cycle "Sécurité Numérique" à l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ)

M. Olivier KEMPF, maître de conférences à l'Institut d'études politiques de Paris

M. Daniel VENTRE, ingénieur CNRS, titulaire de la chaire cyberdéfense et cybersécurité des écoles de Saint-Cyr Coëtquidan

ANNEXE II -

LISTE DES DÉPLACEMENTS

● À Berlin (le 19 janvier 2012)

M. HEISS, directeur à la chancellerie fédérale, en charge du contrôle politique et administratif du service de renseignement extérieur (BND) et coordinateur du renseignement au niveau fédéral

Mme Cornelia REGALL-GROTHE, Secrétaire d'état du ministère fédéral de l'intérieur (BMI), chargée de mission gouvernementale des systèmes d'information

Son Exc. M. Maurice GOURDAULT-MONTAGNE, Ambassadeur de France en Allemagne

Général Philippe CHALMEL, attaché de défense, M. Patrick LEFORT, attaché de défense adjoint et lieutenant-colonel de gendarmerie CHAMBON, attaché de sécurité intérieur adjoint

● À Londres (le 31 janvier-1er février 2012)

M. Gerald HOWARTH, membre du Parlement, Secrétaire d'Etat auprès du ministre de la Défense, ministre chargé de la stratégie internationale de sécurité

M. James ARBUTHNOT, membre du Parlement, Président de la commission de la défense de la Chambre des Communes ;

Lord TEVERSON, membre du Parlement, Président de la sous-commission des affaires européennes, des affaires étrangères, de la défense et de la coopération de la Chambre des Lords ;

Mme Pauline NEVILLE-JONES, ancien ministre de la Sécurité

M. James QUINAULT, Director of Cyber Security & Information Assurance et M. Martin HOWARD, Deputy Information, Security and Assurance (CESG/GCHQ)

Amiral Alan William John WEST, Ancien ministre de la Sécurité

Son Exc. M. Bernard EMIE, Ambassadeur de France au Royaume-Uni ;

Vice-amiral Charles-Edouard de CORIOLIS, attaché de défense

M. Antoine ANFRE, Ministre-conseiller et M. Xavier CHATEL, Premier Secrétaire à l'ambassade de France à Londres

● À Bruxelles, auprès de l'OTAN (le 13 février 2012)

M. Gabor IKLODY, Secrétaire général adjoint de l'OTAN pour les défis émergents de sécurité, en charge notamment des questions de cybersécurité, et M. Suleyman ANIL, spécialiste de la cyberdéfense à l'OTAN

Lieutenant général Kurt HERRMANN, directeur de l'agence de l'OTAN pour les systèmes de services d'information et de communication (NCSA)

M. Jim SIMON, Microsoft.

Son Exc. M. Philippe ERRERA, Ambassadeur, Représentant permanent de la France auprès de l'OTAN ;

Mme Paola DEBRIL-LOISEAU, conseillère des affaires étrangères et M. Jean-Christophe LENFANT, ingénieur en chef de l'armement, chargés de la cyberdéfense à la représentation permanente de la France auprès de l'OTAN

● À Tallinn, en Estonie (le 28 mai 2012)

M. Mikk MARRAN, Secrétaire général du Ministère de la Défense

M. Jaan PRIISALU, Directeur de l'Agence nationale des systèmes d'information (RIA)

colonel Ilmar TAMM, Commandant du Centre d'excellence pour la cyberdéfense en coopération à Tallinn

Son Exc. M. Frédéric BILLET, Ambassadeur de France en Estonie

Mme Hélène ROOS, Adjointe du chef de poste

● À Bruxelles, auprès de l'Union européenne (le 13 juin 2012)

Général Ton VAN OSCH, directeur général de l'Etat-major de l'Union européenne ;

M. Robert MADELIN, Directeur général de la DG Société de l'information et médias de la Commission européenne ;

Son Exc. M. Jean-Louis FALCONI, Ambassadeur, Représentant permanent de la France auprès du COPS ;

Son Exc. M. Philippe ETIENNE, Ambassadeur, Représentant permanent de la France auprès de l'Union européenne ;

Mme Natacha WAKSMAN, M. Romain BONENFANT et M. Ziad KHOURY, conseillers à la représentation permanente de la France auprès de l'Union européenne ;

● À Washington (les 18 et 19 juin 2012)

M. Steven SCHLEIEN, Principal Director cyber policy, Office of Secretary of Defense (OSD), département de la défense (*Department of Defense*)

Mme Jordana SIEGEL, Directeur des affaires stratégiques et internationales du *National Protection and Programs Division* et M.Amit KHOSLA, agent du *National and Cybersecurity and Communication Integration Center (NCCIC),* du Département de la sécurité intérieure (*Department of Homeland Security*)

M. James LEWIS, Director and Senior Fellow, Technology and Public Policy Program, expert au *Center for Strategic and International Studies* (CSIS)

M. Christopher PAINTER, Coordonnateur Cyber au Département d'Etat

Visite du *Defense Cyber Crime Center* (DC3) du département de la défense et entretien avec M. Steven SHIRLEY, Executive Director, et M. James CHRISTY, chef de division

Visite de l'Agence de sécurité nationale (*National Security Agency*) (NSA) et entretien avec M. Dennis BARTKO, Director's special Assistant for Cyber et M. Adrian LAPOINTE, Special Assistant to the Director of Foreign Affairs for Cyber

M. Ted DEUTCH, représentant (démocrate) de Floride, membre de la commission des affaires étrangères, M. Alcee HASTINGS, représentant (démocrate) de Floride, M. Jim LANGEVIN, représentant (démocrate) de Rhodes-Island, co-président de la commission parlementaire sur la cybersécurité, M. Roscoe BARTLETT, représentant (républicain) du Maryland, membre de la commission parlementaire sur la cybersécurité, M. Eliot ENGEL, représentant (démocrate) de New-York, membres de la Chambre des représentants du Congrès des Etats-Unis

Son Exc. M. François DELATTRE, Ambassadeur de France aux Etats-Unis,

Général Bruno CAÏTUCOLI, attaché de défense, colonel Michel DUPONT, attaché de défense adjoint, commandant Arnaud BALESTE, attaché de sécurité adjoint, M. Eric KOBAK, attaché de l'armement adjoint, Mme Emmanuelle PAVILLON, chef de cabinet et Mme Pia DECARSIN, rédactrice au service de presse et de communication de l'ambassade de France aux Etats-Unis

Dîner de travail sur la cyberdéfense, organisé par le *German Marshall Fund,* en présence de représentants des autorités, d'experts et d'universitaires

ANNEXE III - GLOSSAIRE

1. Termes techniques

botnet : un *botnet*, autrement dit un « réseau de robots », est un réseau d'équipements compromis (ordinateurs, serveurs, ordiphones, etc.) à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du *botnet* et de les actionner à sa guise, par exemple pour envoyer des courriers électroniques non désirés ou pour lancer des attaques par déni de service

BYOD (*bring your own device* ou "apporter son propre terminal") : pratique consistant à utiliser son ordinateur personnel, sa tablette ou son ordiphone dans un cadre professionnel.

bombe programmée, bombe logique (*logic bomb) :* logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies.

canal caché (*covert chanel*) : canal de communication qui permet à un processus malveillant de transférer des informations d'une manière dissimulée.

cheval de Troie : dans le domaine informatique, le cheval de Troie ouvre un accès dissimulé qui permet à un utilisateur malveillant de prendre le contrôle de l'ordinateur compromis et de s'en servir à l'insu de propriétaire.

cloud computing ou **informatique en nuage :** pratique consistant à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur. Ce système permet notamment à des utilisateurs et des entreprises de délocaliser et de mutualiser la gestion de leur système informatique.

code malveillant (*malware*) : tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Les virus, les vers ou les « chevaux de Troie » sont des types de codes malveillants.

defacement : voir défiguration.

défiguration (*defacement*) : résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur internet, et a donc violé l'intégrité des pages en les altérant.

déni de service : action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

déni de service distribué : action ne déni de service lancée depuis plusieurs sources.

DDoS (***Distributed denial of service***) : voir déni de service distribué.

DoS (***Denial of service***) : voir déni de service.

élévation de privilège (*privilege escalation*) : obtention de privilège supérieur par exploitation d'une vulnérabilité. Des codes malveillants peuvent ainsi se faire attribuer des facultés d'administration

enregistreur de frappe (*keylogger*) : logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne saisi à partir de son clavier.

firewall : voir pare-feu.

hacker : pirate informatique.

IP ou *internet protocol* : la communication sur l'internet est fondée sur un protocole appelé IP pour *internet protocol* qui permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la communication en paquets comportant chacun une adresse de source et une adresse de destination.

keylogger : voir enregistreur de frappe.

logiciel espion (*spyware*) : logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

mail bombing : bombardement de courriels : envoi d'une grande quantité de courriels à un destinataire unique dans une intention malveillante.

malware : voir code malveillant.

man-in-the-middle : « homme-au-milieu » : catégorie d'attaque où une personne malveillante s'interpose dans une session de communication de manière transparente pour les utilisateurs ou les systèmes.

outil de dissimulation d'activité (*rootkit*) : tout programme ou ensemble de programmes placé au plus près du système d'exploitation et permettant de dissimuler une activité, malveillante ou non, sur une machine. Par extension, tout programme ou ensemble de programmes permettant à une personne malveillante de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités.

pare-feu (*firewall*) : un pare-feu est un logiciel ou un équipement permettant de protéger un ordinateur ou un ensemble d'ordinateurs connectés à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

pourriel (*spam*) : tout courrier électronique non sollicité par le destinataire.

porte dérobée *(backdoor)* : accès dissimulé qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive. Des portes dérobées peuvent exister dans les logiciels (systèmes d'exploitation ou applications) ou dans les composants d'un équipement (ordinateurs, ordiphones, etc.)

rétroconception : processus d'analyse d'un composant informatique, par exemple un logiciel, visant à en reconstruire les spécifications techniques et fonctionnelles.

routeur : Les « routeurs » sont des grands équipements d'interconnexion de réseaux informatiques utilisés notamment par les opérateurs de télécommunications qui permettent d'assurer le flux des paquets de données entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

rootkit : voir outil de dissimulation d'activité.

spam : voir pourriel.

spyware : voir logiciel espion.

ver : logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis à l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Les vers sont des catégories de virus, qui se propagent de manière quasi-autonome et dont le vecteur primaire de propagation reste le réseau. Ils peuvent être également transmis par cléUSB (comme les vers Conficker ou Stuxnet).

virus : programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et souvent d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau).

zombie : équipement informatique (ordinateur, serveur, etc.) compromis inclus dans un réseau (botnet) contrôlé par un individu malveillant.

2. Sigles et abréviations

ANSSI : Agence nationale de la sécurité des systèmes d'information (Premier ministre)

AQSSI : autorité qualifiée en sécurité des systèmes d'information

BSI : *Bundesamt für Sicherheit in des Informationstechnik* (service homologue de l'ANSSI en Allemagne)

CALID : Centre d'analyse de lutte informatique défensive (ministère de la défense)

CDMA : *NATO Cyber Defense Management Authority* (OTAN)

CERT – *Computer emergency response team* (équipe de réponse aux attaques informatiques)

CESG : *Communications and electronic security group* (service correspondant de l'ANSSI au Royaume-Uni)

COSSI : Centre opérationnel de la sécurité des systèmes d'information (ANSSI)

DISIC : Direction interministérielle des systèmes d'information et de communication de l'Etat (Premier ministre)

DGSIC : Direction générale des systèmes d'information et de communication (ministère de la défense)

EGC : *European Government Computer Security Incident Response Teams* (groupe réunissant huit CERT gouvernementaux européens)

ENISA : *European Network and Information Security Agency* (agence de l'Union européenne en charge de la sécurité des systèmes d'information

FIRST : *Forum of incident response and security teams* (enceinte internationale regroupant les CERT)

FSSI : fonctionnaire de sécurité des systèmes d'information

IVBB : Informationverbund Berlin-Bonn (réseau de communication gouvernemental allemand)

ISIS : intranet sécurisé interministériel pour la synergie gouvernementale

NCIRC : *NATO Computer incident response capability* (OTAN)

OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (ministère de l'intérieur – direction centrale de la police judiciaire)

OIV : opérateur d'importance vitale

OPVAR : organisation permanente veille, alerte, réponse

RGS : référentiel général de sécurité

RIE : Réseau interministériel de l'Etat

RGS : Référentiel général de sécurité

RSSI : responsable de la sécurité des systèmes d'information

SCADA : *Supervisory, control and data acquisition* (systèmes de supervision et de régulation)