N° 449

SÉNAT

SESSION EXTRAORDINAIRE DE 2007-2008

Annexe au procès-verbal de la séance du 8 juillet 2008

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. Roger ROMANI,

Sénateur.

(1) Cette commission est composée de : M. Josselin de Rohan*, président ;* MM. Jean François-Poncet, Robert del Picchia, Jacques Blanc, Mme Monique Cerisier-ben Guiga, MM. Jean-Pierre Plancade, Philippe Nogrix, André Boyer, Robert Hue*, vice-présidents ;* MM. Jacques Peyrat, Jean-Guy Branger, Jean-Louis Carrère, André Rouvière, André Trillard*, secrétaires ;* MM. Bernard Barraux, Jean-Michel Baylet, Mme Maryse Bergé-Lavigne, MM. Pierre Biarnès, Didier Borotra, Didier Boulaud, Robert Bret, Mme Paulette Brisepierre, M. Christian Cambon, Mme Michelle Demessine, M. André Dulait, Mme Josette Durrieu, MM. Jean Faure, Jean-Pierre Fourcade, Mmes Joëlle Garriaud-Maylam, Gisèle Gautier, Nathalie Goulet, MM. Jean-Noël Guérini, Michel Guerry, Hubert Haenel, Joseph Kergueris, Robert Laufoaulu, Louis Le Pensec, Simon Loueckhote, Philippe Madrelle, Pierre Mauroy, Louis Mermaz, Mme Lucette Michaux-Chevry, MM. Charles Pasqua, Daniel Percheron, Xavier Pintat, Yves Pozzo di Borgo, Jean Puech, Jean-Pierre Raffarin, Yves Rispat, Roger Romani, Gérard Roujas, Mme Catherine Tasca, M. André Vantomme, Mme Dominique Voynet.

S O M M A I R E

Pages

Mesdames, Messieurs,

Au **printemps 2007**, alors qu'une vive tension diplomatique l'oppose à la Russie, **l'Estonie est victime d'une attaque massive contre les sites internet du gouvernement, des banques et des opérateurs téléphoniques**. Leur fonctionnement est altéré durant plusieurs semaines, provoquant d'importantes perturbations dans un pays où les communications électroniques sont particulièrement utilisées dans la vie courante.

Quelques semaines plus tard, en **septembre 2007**, **les autorités françaises révèlent que des services de l'Etat ont fait l'objet d'attaques ciblées visant à s'introduire dans leurs systèmes d'information, vraisemblablement à des fins d'espionnage**. Ces tentatives proviennent de Chine sans qu'il soit possible d'en établir précisément l'origine. Plusieurs autres pays – Etats-Unis, Royaume-Uni, Allemagne, Nouvelle-Zélande – font eux aussi état d'attaques analogues ayant touché leurs systèmes gouvernementaux sur la même période.

La vulnérabilité des réseaux informatiques n'est pas une préoccupation nouvelle dans des sociétés devenues très étroitement dépendantes du bon fonctionnement de leurs systèmes d'information. Les signes d'actions mettant directement en cause la sécurité de systèmes gouvernementaux ou stratégiques sont apparus aux Etats-Unis dès le début de la décennie, mais les incidents survenus en Europe l'an passé, largement médiatisés, ont matérialisé de manière très concrète une **menace encore mal identifiée** sur notre continent, **particulièrement en France**.

Les **insuffisances de notre pays** dans la prise en compte de cette menace avaient été **soulignées lors du lancement du plan triennal de renforcement de la sécurité des systèmes d'information de l'Etat**, en mars 2004, puis dans le **rapport remis au Premier ministre en janvier 2006** par notre collègue député **Pierre Lasbordes**.

Votre commission des Affaires étrangères, de la défense et des forces armées a considéré que les enjeux liés la sécurité des systèmes d'information, du point de vue de la défense et de la sécurité nationale, ne pouvaient qu'aller en s'accentuant. Aussi a-t-elle décidé au mois de février dernier de préparer un rapport d'information sur un sujet dont le Livre blanc, rendu public le 17 juin dernier, souligne lui aussi le caractère stratégique.

Le présent rapport d'information n'a pas pour ambition de traiter l'ensemble de la problématique de la sécurité des systèmes d'information, qui concerne tout autant le simple particulier que les organismes d'Etat et couvre un champ allant de la simple malveillance ou de l'escroquerie, à des actions à visées politiques ou stratégiques.

Il s'intéresse essentiellement aux **atteintes portées aux systèmes d'information susceptibles de mettre en cause la sécurité et la défense du pays** et aux **moyens de s'en protéger**, que l'on a résumé pour simplifier sous le vocable de « cyberdéfense ».

S'appuyant sur les témoignages recueillis auprès des responsables des services de l'Etat ou d'entreprises particulièrement concernées, ce rapport vise à mieux comprendre la façon dont ces atteintes pourraient se manifester et les conséquences qu'elles pourraient entraîner, à évaluer les réponses qui sont mises en place par les pouvoirs publics et à dégager quelques axes sur lesquels une accentuation de l'effort paraît indispensable.

Votre rapporteur a tout d'abord souhaité illustrer, au travers des exemples récents, **la nature et les formes que pourrait revêtir cette menace**. La neutralisation de certains systèmes d'informations critiques pour la vie de la nation ou leur pénétration en vue d'en altérer ou détourner les données, figurent parmi les objectifs potentiels d'éventuels agresseurs. L'ouverture des réseaux vers l'extérieur les rend vulnérables aux entreprises de plus en plus élaborées de spécialistes qui perfectionnent de jour en jour leur savoir-faire.

Il a ensuite constaté que **malgré des efforts réels, la France restait encore insuffisamment préparée et organisée** face à la menace d'attaques informatiques. 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, votre rapporteur détaille les **orientations très positives retenues par le Livre blanc**, qui élève la **protection des systèmes d'information** au rang de **composante à part entière de notre politique de défense et de sécurité**. Les instruments évoqués par le Livre blanc, notamment la future Agence de la sécurité des systèmes d'information, devront toutefois être impérativement dotés des moyens et de l'autorité permettant de mener une action plus résolue dans le domaine de la sécurité des systèmes d'information. Votre rapporteur formule plusieurs propositions en ce sens.

I. LA PROTECTION DES SYSTÈMES D'INFORMATION : UN VÉRITABLE ENJEU DE SÉCURITÉ NATIONALE

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 codes d'accès ou les coordonnées bancaires de l'utilisateur.

La perception d'un **risque pesant plus particulièrement sur la sécurité des Etats** est principalement apparue aux Etats-Unis il y a une dizaine d'années, avec l'identification de tentatives de pénétration et d'attaques de saturation sur les systèmes d'agences gouvernementales, de centres de recherche ou d'entreprises sensibles.

Elle est aujourd'hui largement partagée dans les pays industrialisés. On y mesure désormais que le développement considérable des systèmes d'information, dont nos sociétés sont devenues extrêmement dépendantes, et leur interconnexion croissante, ont souvent été réalisés au détriment des exigences de sécurité qui constituent en la matière une contrainte incontestable.

Deux grandes séries de préoccupations émergent.

La première porte sur les **services essentiels au fonctionnement du pays ou à sa défense**, tributaires de systèmes informatiques 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.

Certes, dans un cas comme dans l'autre, un adversaire potentiel dispose d'une multitude de moyens pour parvenir à ses fins : destruction physique d'une infrastructure, utilisation de complicités internes ou modes classiques d'acquisition du renseignement. Toutefois, 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.

Les attaques massives de saturation dont ont été victimes de nombreux sites officiels en Estonie au printemps 2007, tout comme les attaques plus ciblées provenant de Chine et constatées, au cours de la même période, en France et dans plusieurs pays occidentaux, constituent une manifestation concrète de cette menace.

Aux yeux de votre rapporteur, la relative modestie des investissements nécessaires pour mener de telles attaques et la possibilité d'en masquer facilement l'origine rendent très probable leur développement dans les années à venir.

A. UNE MENACE AUX MANIFESTATIONS DE PLUS EN PLUS ÉVIDENTES

Avant de tenter de dresser une typologie des attaques informatiques, des méthodes utilisées et des cibles potentielles, il paraît nécessaire à votre rapporteur de détailler la façon dont elles se sont récemment manifestées en Europe.

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**, suite à la décision des autorités de Tallin de déplacer du centre de la ville vers un cimetière militaire le monument érigé en souvenir des combattants de l'armée soviétique qui avaient mis fin à l'occupation allemande en 1944. 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 visant les sites gouvernementaux et publics, ceux des opérateurs de téléphonie mobile, des banques commerciales et des organes d'information**.

Ces attaques par « **déni de service** » (*Denial of service – DOS*) visaient à **saturer, par une multitude de demandes de connections simultanées, les sites concernés**. Ceux-ci se trouvaient de ce fait inaccessibles.

Les perturbations se sont poursuivies sur 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 connections par seconde.

La technique utilisée pour ces attaques est celle des **« réseaux de robots** » (*botnets*) constitués d'ordinateurs compromis à l'insu de leur propriétaire, et actionnés par l'auteur de l'attaque qui usurpe ainsi leur identité.

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 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 parfaitement coordonné, ce qui conduit à exclure la seule action d'individus isolés agissant par motivation politique et utilisant des consignes trouvées sur certains sites internet. L'essentiel de l'attaque provenait de réseaux de robots (*botnets*) contrôlés par des organisations criminelles qui en monnayent l'utilisation.

La particularité de telles attaques est qu'il est **impossible d'en identifier les auteurs**. On ne peut 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. Pour l'heure, seul un jeune étudiant estonien russophone a été identifié comme ayant pris part aux attaques et condamné.

Le cas estonien illustre cependant 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.

2. Les « attaques chinoises » du printemps 2007 : une tentative de pénétration des systèmes d'information gouvernementaux

Les Etats-Unis avaient révélé à plusieurs reprises avoir fait l'objet de tentatives de pénétration de leurs systèmes d'information par des éléments étrangers. En 1998 et 1999, une vague d'attaque baptisée « *Moonlight Maze* » et supposée d'origine russe avait ciblé les systèmes gouvernementaux ainsi que ceux de centres de recherche et d'entreprises sensibles. Une autre offensive dénommée « *Titan Rain* », utilisant des réseaux chinois, a quant à elle démarré en 2001 et visé le Département de la défense durant plusieurs années, certaines tentatives d'intrusion ayant semble-t-il été couronnées de succès.

Les **attaques dites « chinoises »,** dont plusieurs gouvernements occidentaux ont indiqué avoir été la cible **au cours des années 2006 et 2007**, font référence à des tentatives menées dans plusieurs pays selon un mode opératoire identique : l'envoi à des hauts responsables ou des fonctionnaires, ainsi qu'à des dirigeants d'entreprises, de **courriers électroniques apparemment légitimes**, mais dont la **pièce jointe, piégée, comportait un « cheval de Troie »**, c'est-à-dire un programme informatique permettant de prendre le contrôle d'un ordinateur et de s'en servir à l'insu de son utilisateur.

En **France**, ces attaques ont visé le ministère des Affaires étrangères, et en particulier des diplomates en poste en ambassade. Elles se présentaient

sous la forme de messages anodins, en relation avec l'actualité ou les centres d'intérêt des destinataires. La pièce jointe était susceptible d'installer sur l'ordinateur visé un programme forgé spécifiquement, et donc non détectable par les protections habituelles (pare-feux ; anti-virus), dans un but de récupération et de transfert des informations vers un serveur étranger.

Les autorités françaises ont indiqué que **ces attaques avaient transité par la Chine**, tout en restant prudentes sur leur origine exacte qui n'a 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.

Il est à noter que lors de la présentation de son dernier bilan sur la maîtrise des risques publié au mois de juin, le **Commissariat à l'énergie atomique (CEA)** a donné des indications précises sur les attaques informatiques dont il a fait l'objet en 2007, en soulignant que les attaques aveugles et récurrentes marquaient le pas au profit d'**attaques plus ponctuelles dans le temps** (de quelques heures à quelques jours) et **plus précises en termes de cibles visées**. La diversité de ces infections met en défaut les systèmes de détection classiques qui travaillent sur la base d'attaques connues. Le CEA a indiqué que ces attaques provenaient fréquemment de Chine.

Dans le même temps, plusieurs autres pays ont indiqué avoir été victimes d'attaques de même type, impliquant elles aussi des serveurs chinois.

Aux **Etats-Unis**, des intrusions ont été détectées sur les **systèmes d'information du département de la défense**, et plus particulièrement sur les serveurs de messageries. Une partie du réseau informatique directement lié au secrétaire à la défense a dû être mise hors service durant plusieurs jours.

Des faits de même nature ont été signalés en **Allemagne**, où les services de renseignement auraient bloqué un important volume de données provenant des systèmes d'information gouvernementaux qui étaient en passe d'être transférées vers des serveurs localisés en Chine. Au **Royaume-Uni**, le *Foreign office* a été affecté, de même que des systèmes gouvernementaux en Australie, en Nouvelle-Zélande, au Canada, en Suisse, en Belgique ou aux Pays-Bas.

Il est difficile de ne pas effectuer un **rapprochement entre toutes ces tentatives d'intrusion** qui se sont déroulées sur la même période, ont visé des cibles de même nature et ont utilisé, selon les informations recueillies par votre rapporteur, une quinzaine de types de courriers électroniques piégés utilisant des codes malveillants spécialement mis au point. Ceux-ci ont paru suffisamment sophistiqués pour laisser penser qu'ils **ne sont pas l'œuvre d'individus isolés, mais de groupes organisés**, voire de services de renseignement.

L'implication de **pirates informatiques** (« *hackers* ») **tolérés et contrôlés par les autorités chinoises**, voire de l'armée populaire de libération chinoise elle-même, a été immédiatement évoquée. Depuis plusieurs années, les agissements de ces groupes sont mis en cause par les autorités américaines, ainsi que par Taïwan, qui considère que ses organes gouvernementaux et ses grandes entreprises font l'objet d'un espionnage électronique incessant par la Chine continentale. Les autorités chinoises ont démenti tout lien avec ces évènements et indiqué être elles-mêmes confrontées aux agissements de pirates informatiques contre les systèmes gouvernementaux.

Qu'elles aient prioritairement visé à détourner des informations sensibles ou qu'elles aient surtout été effectuées pour tester la protection des systèmes informatiques visés, ces attaques démontrent néanmoins la **banalisation de l'usage de techniques informatiques peu détectables comme arme de renseignement**.

B. UNE MENACE AUX FORMES MULTIPLES

Le **déni de service**, qui vise à stopper le fonctionnement d'un système informatique, et l'**intrusion en vue de détourner des informations** constituent les deux principales formes de menaces pesant sur les systèmes gouvernementaux ou d'entreprises sensibles.

L'**usage des technologies informatiques** apparaît comme une **alternative au recours à des méthodes plus traditionnelles**, telles que la destruction, le brouillage par rayonnement électromagnétique, l'intrusion physique ou le contrôle de sources de renseignement internes.

Les conséquences de telles attaques doivent être distinguées selon qu'elles se limitent à rendre indisponibles des sites d'information ou des services en ligne accessibles au grand public, ou qu'elles atteignent plus directement le réseau interne d'institutions ou d'entreprises.

Enfin, ces attaques s'appuient de plus en plus sur des **communautés de pirates informatiques** susceptibles d'offrir leurs services à des organisations criminelles comme à des Etats, ce qui n'exclut pas la mise en place par ces derniers de leurs propres moyens offensifs.

1. Les principaux types d'attaques informatiques

Par distinction avec les actes délictueux commis par des individus isolés et les activités frauduleuses de réseaux se livrant à la « cybercriminalité », on a pu parler de véritable **guerre informatique** pour caractériser les actions visant à paralyser les systèmes d'une institution ou d'une entreprise, ou à en détourner ou déformer les données.

De manière générale, on distingue **trois modes principaux de guerre informatique** :

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

- 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 par l'information, qui utilise le vecteur informatique dans un but de propagande, de désinformation ou d'action politique.

Votre rapporteur évoquera ici plus particulièrement les principales formes d'attaques constatées au cours de la période récente, à savoir les actions par déni de service et le vol ou l'altération de données.

● ***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. 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. Les évènements d'Estonie 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*** (réseaux de « robots » logiciels) constituent le vecteur privilégié de ces attaques. Ces réseaux de machines compromises (ou machines « zombies ») 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. 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*).

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. Enfin, 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.

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 constitue un risque supplémentaire 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.

2. Les cibles potentielles

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.

Provoquer l'indisponibilité du site internet d'une institution ou d'une administration, comme on l'a vu en Estonie, 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.

● ***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.

Aux yeux de votre rapporteur, 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.

Votre rapporteur a pu constater, au cours de ses auditions, que ce type de vulnérabilité potentielle avait été pleinement pris en compte par une entreprise comme **EDF** pour la gestion de la production et de la distribution électrique. Celle-ci applique un niveau de sécurité très élevé pour ses applications informatiques de nature industrielle, qu'elle a totalement isolées des autres réseaux internes et qu'elle soumet à des procédures très strictes en matière d'accès, d'identification et de surveillance.

Les systèmes de type SCADA peuvent également être utilisés dans d'autres types d'activités industrielles moins vitales. Une protection insuffisante peut conduire à les exposer aux agressions extérieures et en perturber le fonctionnement.

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.

Dès lors, il paraît clair que la **lutte informatique** va inévitablement devenir un **nouveau compartiment du champ de bataille**, avec ses aspects défensifs et offensifs, comme l'était déjà le domaine de la guerre électronique.

● ***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** visant à cibler, par les techniques qui ont été mentionnées plus haut (notamment les chevaux de Troie), 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, militaire, économique, scientifique, technologique ou industriel.

3. Le profil des « attaquants » : pirates informatiques, terroristes, services étatiques ?

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 différents. 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 »***

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** (*hackers*) agissant en groupes et essentiellement motivés par l'appât du gain. 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.

On considère que ces groupes 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 émanant de pirates chinois et dirigées contre les Etats-Unis ou Taïwan.

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

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 agissent également depuis les Etats-Unis. Enfin, les groupes de pirates les plus importants et actifs seraient situés en Chine. On notamment été cités la « *Red Hacker's Alliance* » qui, selon la presse de Taïwan, compterait près de 20 000 membres, le groupe « *Titan Rain* », impliqué dans les attaques survenues aux Etats-Unis en 2001, ou la « *China Eagle Union* ».

● ***Vers un « 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 récemment 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.

● ***L'implication des Etats : le cas de la Chine***

Si nombre de services de renseignement entretiennent une compétence offensive dans le domaine informatique, ne serait-ce qu'en matière d'écoute passive des flux d'information, leur implication dans des attaques n'a jamais été avérée.

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.

Selon 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. 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 mentionnés ci-dessus. L'internet est très étroitement contrôlé par les autorités chinoises qui disposent de ce fait d'un important moyen de pression sur ces groupes.

C. UNE MENACE QUI NE PEUT ALLER QU'EN S'ACCENTUANT

Aux yeux de votre rapporteur, il n'est pas douteux que les évènements survenus en Estonie ou les attaques dites « chinoises » opérées contre plusieurs Etats européens ne sont que de premières manifestations d'un **phénomène appelé à s'accentuer**, et ce pour au moins trois raisons.

Premièrement, il est banal de souligner que **les systèmes d'information et l'internet** prennent une place chaque jour grandissante dans tous les domaines de la vie et du fonctionnement de nos sociétés, devenant de ce fait une **cible potentielle**. Il est en effet particulièrement tentant pour un agresseur, qu'il s'agisse d'un groupe non étatique ou d'un Etat, d'utiliser l'arme informatique pour perturber la vie courante, générer des troubles, accéder à des informations sensibles du point de vue politique, économique et militaire, et amoindrir nos capacités d'action.

Deuxièmement, ce **mode opératoire** est **relativement accessible et « rentable »**. Il s'appuie sur des technologies dont la maîtrise n'est pas réservée à un nombre limité de spécialistes ou à des organisations étatiques. L'ouverture et l'interconnexion croissantes des réseaux, de même que la généralisation de produits standards dont les vulnérabilités sont en permanence scrutées par les communautés de pirates informatiques, en facilitent l'usage. Il s'avère relativement peu coûteux et s'affranchit très facilement des distances et des frontières. Le volume considérable du courrier électronique non sollicité (*spams*), qui dépasse souvent plus de 95 % du trafic dirigé vers les administrations et les entreprises, illustre l'effet démultiplicateur des techniques dont disposent des agresseurs, même si la plus large part de ces envois ne présente pas de risque de sécurité majeur.

Enfin, l'attaque informatique est particulièrement **difficile à identifier**. Elle procède par rebonds utilisant une succession d'adresses relais et permet de cacher ou de déguiser son identité. Le transit par un grand nombre de pays entrave les possibilités d'enquête, et s'il est possible de localiser le serveur, les législations locales permettent rarement de remonter jusqu'à l'initiateur de l'attaque. L'utilisation éventuelle d'ordinateurs situés dans des sites publics, comme les cybercafés, peut aussi faire obstacle à l'identification. Enfin, le lien entre les pirates informatiques et leurs commanditaires reste le plus souvent impossible à établir avec certitude.

II. LA FRANCE EST ENCORE INSUFFISAMMENT PRÉPARÉE ET ORGANISÉE

Si la France a atteint un haut degré dans la diffusion et l'usage des systèmes d'information, elle n'a sans doute pas accordé suffisamment d'importance à la sécurité de ces systèmes.

Les exigences de sécurité paraissent encore trop souvent considérées comme une source de contraintes excessives, allant à l'encontre de solutions techniques plus simples et plus efficaces pour l'opérateur et pour l'utilisateur.

Quant aux activités d'ingérence ou d'espionnage par voie informatique, elles suscitent parfois l'étonnement ou le scepticisme. Que ce soit dans les services de l'Etat ou le monde de l'entreprise, la conscience de pouvoir devenir la cible d'une telle menace n'est guère répandue, du moins tant qu'elle ne s'est pas concrètement matérialisée. Cette situation renvoie d'une certaine manière au constat sur les insuffisances de la « culture du renseignement » et de la sensibilisation aux enjeux de l'intelligence économique dans notre pays, par rapport à certains de nos partenaires, notamment anglo-saxons.

Les politiques publiques en matière de sécurité des systèmes d'information ont été lancées il y a une vingtaine d'années, mais leurs limites ont conduit en 2004 le Premier ministre de l'époque à définir un plan triennal de renforcement de la sécurité des systèmes d'information de l'Etat. Une **analyse exhaustive de la situation de la France au regard de la sécurité des systèmes d'information** a été publiée au début de l'année 2006, dans le cadre de la mission qui avait été confiée à notre collègue député **Pierre Lasbordes**. Le rapport de ce dernier dresse un **constat sévère**, tant en termes d'organisation que de moyens. En effet, si des avancées incontestables ont été effectuées ces dernières années, elles demeurent insuffisantes au regard des enjeux.

La France accuse ainsi un **réel retard par rapport à nos principaux partenaires, en premier lieu l'Allemagne et le Royaume-Uni**.

Enfin, la France participe à diverses enceintes internationales dans ce domaine, mais les coopérations en sont encore à un stade peu développé, notamment en ce qui concerne l'Union européenne.

A. UNE PRISE DE CONSCIENCE RÉCENTE ET DES POLITIQUES TROP TIMIDES

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

pour la sécurité des services d'information, ainsi que d'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. Succédant au service central précédemment mentionné, la **Direction centrale de la sécurité des services d'information (DCSSI)**, partie intégrante du SGDN, a été créée par décret du 31 juillet 2001. Elle est chargée d'apporter son soutien à l'ensemble des administrations par des missions d'inspection et de conseil. Elle évalue et vérifie la sécurité des réseaux et des systèmes d'information des services publics. Elle agrée tous les matériels de chiffrement qui protègent des données classifiées. Elle prépare et met en œuvre les mesures de sécurité des systèmes d'information prévues par les plans Vigipirate et Piranet.

Outre cette structure interministérielle, **plusieurs ministères disposent de compétences spécifiques** intéressant la sécurité des systèmes d'information : le **ministère de la défense**, avec la Délégation générale pour l'armement, au travers de son expertise technique (notamment le CELAR, Centre électronique de l'armement), 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 de la surveillance du territoire (DST), devenue Direction centrale du renseignement intérieur (DCRI), et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) ; les ministères de l'économie et des finances et du budget, avec les structures de soutien à l'innovation et la Direction générale de la modernisation des moyens de l'Etat, qui a notamment repris les attributions de l'Agence de développement de l'administration électronique (ADAE).

Enfin, **chaque ministère est responsable de la sécurité de ses propres systèmes d'information**. L'organisation retenue repose sur les hauts fonctionnaires de défense placés auprès de chaque ministre, éventuellement assistés d'un fonctionnaire de sécurité des systèmes d'information (FSSI). Aux différents échelons des administrations centrales et des services déconcentrés doivent être désignées des autorités qualifiées en sécurité des systèmes d'information (AQSSI)

Au cours de ses auditions, votre rapporteur a constaté un **sentiment très largement partagé de nécessaire réforme de ce dispositif**, tant en termes d'organisation que de moyens. Le constat sévère effectué il y a un peu plus de deux ans par le rapport Lasbordes n'est guère contesté, même s'il ne faut certainement pas négliger la réalité des efforts qui ont été accomplis, mais restent modestes au regard des besoins.

1. Le constat sévère du rapport Lasbordes de 2006 : un retard préoccupant

Le **plan de renforcement de la sécurité des systèmes d'information de l'Etat,** décidé par le Premier ministre Jean-Pierre Raffarin et exposé dans un document du 10 mars 2004, débute par les considérations suivantes, particulièrement préoccupantes :

« ***Depuis plusieurs années, les rapports annuels des départements ministériels sur l'état de la sécurité des systèmes d'information (SSI) font part des difficultés persistantes rencontrées pour améliorer la situation : compétences et capacités opérationnelles trop réduites et isolées, manque de sensibilité des décideurs aux enjeux, insuffisance de produits de sécurité dûment qualifiés combinée à des positions monopolistiques dans des segments importants du marché, prolifération d'interconnexions de réseaux mal sécurisés, réglementation nationale difficilement applicable, dimension européenne mal coordonnée. Si certaines améliorations ponctuelles sont constatées, les efforts accomplis, pour méritoires qu'ils soient, n'ont pas été à la mesure de l'évolution rapide des technologies et des menaces*** ».

En parallèle avec la mise en place du plan destiné à redresser cette situation, M. Jean-Pierre Raffarin décidait le 27 mai 2005 de confier à notre collègue député **Pierre Lasbordes** une **mission sur la sécurité des systèmes d'information**.

Le rapport intitulé : « *La sécurité des systèmes d'information – Un enjeu majeur pour la France* », à la rédaction duquel M. Pierre Lasbordes a associé plusieurs personnalités qualifiées éminentes, a été remis au Premier ministre Dominique de Villepin le 13 janvier 2006.

Le rapport Lasbordes effectue une **analyse exhaustive et approfondie de l'ensemble des enjeux liés à la sécurité des systèmes d'information**, non seulement du point de vue de la protection de l'Etat, mais également de celle des infrastructures vitales et du monde de l'entreprise dans son ensemble.

Il dresse un **constat sans complaisance des faiblesses de notre organisation et de nos moyens**, notamment au regard de nos partenaires européens les plus proches. Il estime 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***». Ce constat, pour l'essentiel, demeure largement valable aujourd'hui.

Le rapport énonce enfin six recommandations générales assorties de propositions détaillées qui, pour la plupart, auraient toujours vocation à être mises en oeuvre.

● ***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 tient à la conduite de la politique de sécurité des systèmes d'information, qui souffre d'une grande dispersion des acteurs et à l'autorité insuffisante des structures chargées de la mettre en œuvre.

Le rapport estime notamment 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*** ».

Le rapport constate que si une **structure interministérielle** existe, elle **n'a pas été investie de l'autorité politique nécessaire pour assurer une véritable coordination des différents acteurs**. On assiste ainsi à des chevauchements de compétence, comme dans le domaine de la labellisation de produits et de procédures. Les prérogatives de la DCSSI relèvent du conseil ou de la recommandation. Elles n'ont pas de caractère directif et ne lui donnent en aucun cas la possibilité d'imposer des prescriptions de sécurité aux différents ministères qui demeurent libres d'appliquer les mesures qui leur semblent pertinentes et adaptées à leurs besoins.

Une **analyse comparative de cinq ministères** montre que la mise en œuvre de la sécurité des systèmes d'information est très hétérogène. Des principes tels que la séparation entre la fonction « sécurité » et les services informatiques, l'identification des logiciels associés aux applications traitant des données sensibles ou la classification de ces données sensibles n'y sont absolument pas appliqués de manière uniforme.

Le rapport relève notamment que le **dispositif de sécurité des systèmes d'information**, reposant sur le haut fonctionnaire de défense et les autorités qualifiées en sécurité des systèmes d'information, est **mis en œuvre de manière très inégale selon les ministères**, et le plus souvent de manière peu satisfaisante. Selon le rapport, « *il est fréquent de constater que les services informatiques ne suivent pas les fortes recommandations des hauts fonctionnaires de défense lors de choix de solutions pour des applications sensibles, sous couvert d'une stricte application du code des marchés publics* ». Il conclut que « *les disparités dans la mise en œuvre de ce dispositif, ainsi que des difficultés à mobiliser des ressources humaines compétentes et dédiées ... et l'absence de pouvoir réel de ces acteurs de la sécurité des systèmes d'information, rendent cette* ***organisation inopérante*** ».

Votre rapporteur s'est intéressé plus particulièrement au **ministère de la défense**, dont les systèmes d'information, par nature, peuvent être la cible

d'actions visant leur disponibilité, leur intégrité ou leur confidentialité. Il a constaté que l'organisation mise en place, résumée dans l'encadré ci-après, prenait en compte de manière cohérente et complète la sécurité des systèmes d'information.

L'organisation de la lutte informatique défensive au ministère de la défense

Le ministère de la défense gère un nombre considérable de systèmes d'information couvrant trois domaines : les systèmes d'information opérationnels et de communication liés à l'emploi des forces ; les systèmes d'information scientifiques et techniques ; les systèmes d'administration et de gestion.

Créée en mai 2006, la **direction générale des systèmes d'information et de communication (DGSIC)** assure le pilotage central de l'ensemble de ces systèmes pour lesquels elle définit une politique commune. Elle comporte une sous-direction de la sécurité des systèmes d'information chargée notamment d'identifier les capacités techniques nécessaires et de conseiller les différentes entités du ministère.

Afin de parer les agressions dont ses systèmes d'information pourraient faire l'objet, le ministère de la défense a mis en place une **organisation permanente, centralisée**, disposant d'une connaissance et d'une vision de l'ensemble des réseaux et devant être en mesure d'assurer en temps contraint, en liaison avec des acteurs identifiés au sein des organismes, les fonctions de :

- **veille**, pour assurer la **prévention** et l'**anticipation** des crises ainsi que la **détection des activités hostiles** ;

- **alerte**, pour analyser, hiérarchiser et **notifier tout évènement présentant un risque** ;

- **réponse**, pour déterminer et conduire les **actions défensives** correspondantes.

Cette **organisation permanente de veille, alerte et réponse** (**OPVAR**) en charge de la lute informatique défensive comprend, à l'échelon central :

- un **comité directeur** qui définit les orientations et fixe les priorités stratégiques ;

- un **centre d'analyse** de lutte informatique défensive (CALID) qui assure la fonction de veille et réalise le volet technique des fonctions d'analyse et de réponse ;

- un **centre opérationnel** situé au centre de planification et de commandement des opérations du ministère, qui décide des réponses appropriées en fonction des éléments techniques fournis par le centre d'analyse et des priorités liées aux missions ;

- une **cellule d'expertise** qui fédère et capitalise l'expertise de l'ensemble des organismes du ministère et des partenaires externes.

Au niveau décentralisé, les actions de lutte informatique défensive sont distribuées aux différents niveaux sous la responsabilité des autorités qualifiées en sécurité des systèmes d'information.

Au cours de ses auditions, il est également apparu à votre rapporteur que l'**absence d'une politique globale et coordonnée** pour la sécurité des systèmes d'information des différents ministères **augmentait la vulnérabilité d'ensemble des réseaux**, leur niveau de sécurisation étant tributaire des maillons les plus fragiles, quelles que soient les dispositifs de sécurité mis en place par ailleurs.

On peut ainsi s'étonner que les **« passerelles » reliant les réseaux des administrations et l'internet** n'aient pas été systématiquement identifiées, comme le prévoyait le plan de renforcement de la sécurité des systèmes d'information de 2004. **La réduction de leur nombre s'impose pour en faciliter la surveillance et diminuer les vulnérabilités**.

A cet égard, le **réseau mis en place par le groupement d'intérêt public RENATER au profit de la communauté française de l'enseignement supérieur et de la recherche** a été présenté à votre rapporteur comme particulièrement **exemplaire**.

Fédérant les grands organismes de recherche[1] et les ministères de l'éducation nationale, de l'enseignement supérieur et de la recherche, RENATER **raccorde plus de 1 000 sites** dispersés sur le territoire national. Il assure l'interconnexion avec une soixantaine d'opérateurs et fournisseurs d'accès internet en France par un **noeud d'échange central** (Sfinx) et dispose de **deux interconnexions** pour les communications avec l'internet dans le reste du monde. Une telle solution, mise en place à l'origine pour disposer de connexions à très hauts débits dans les meilleures conditions de coût, présente des **avantages évidents en matière de sécurité**.

Une telle architecture peut être prise en exemple par des ministères qui n'ont pas eu le même souci de cohérence dans la réalisation de leur réseau.

● ***Des moyens insuffisants***

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

Plaidant pour le maintien et le renforcement d'une base industrielle et technologique et européenne dans le domaine de la sécurité des systèmes d'information, le rapport déplore également la modestie des financements publics en matière de recherche et de soutien à l'innovation.

Il souligne surtout l'**effectif très restreint de la DCSSI**, limité à 100 personnes, qui ne lui permet 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 des responsables de la sécurité des systèmes d'information, de conseil aux administrations et aux entreprises. **Les homologues britannique ou allemand de la DCSSI disposent d'effectifs de quatre à cinq fois supérieurs**.

---

[1] *CEA, CIRAD, CNES, CNRS, INRA, INRIA, INSERM, BRGM, CEMAGREF et IRD*

Aux yeux de votre rapporteur, l'une des manifestations les plus criantes de cette insuffisance de moyens réside dans l'**absence de capacité de surveillance centralisée des flux** transitant entre l'internet et les systèmes d'information des administrations. Il s'agit là d'une **faiblesse majeure par rapport à nos principaux partenaires**, en premier lieu les Allemands, qui disposent d'une telle capacité de surveillance et donc de détection des flux anormaux par lesquels transitent les attaques informatiques.

Dans la situation actuelle, la surveillance et la détection ne peuvent être assurées qu'au niveau de chaque administration. Bien souvent, celles-ci ne disposent pas des moyens humains et de l'expertise technique nécessaire pour accomplir de telles tâches.

Cette lacune capacitaire nous rend dépendants des informations que nos partenaires sont disposés à nous transmettre en cas d'actions telles que celles provenant de Chine l'an passé.

● ***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 retour sur investissement étant dans ce domaine souvent difficilement perceptible.

Il insiste particulièrement sur la **problématique spécifique des PME** qui, bien souvent, ne disposent pas des moyens d'investir dans la sécurité des systèmes d'information, ni de personnels formés et compétents en la matière.

Enfin, le rapport estime que les pouvoirs publics ne répondent que très imparfaitement aux besoins des entreprises qui souhaitent pouvoir disposer d'un interlocuteur unique et de produits certifiés ou labellisés.

Cette situation est préoccupante car les entreprises, y compris celles intervenant dans des domaines sensibles, sont confrontées à la nécessité d'ouvrir de plus en plus leurs réseaux pour communiquer avec leurs partenaires. La généralisation des solutions offertes pour s'adapter à la mobilité de leurs collaborateurs (connexions à distance, usage d'outils mobiles) renforce leur vulnérabilité.

L'adoption par les entreprises d'une politique de sécurité de systèmes d'information adaptée à leurs particularités et au niveau de risque est une nécessité. Votre rapporteur a eu le sentiment, à l'issue de ses auditions, que les craintes émises à ce sujet par le rapport Lasbordes restaient d'actualité.

A titre d'exemple, il lui semble utile de présenter les principes d'action en matière de sécurité des systèmes d'information qui animent un groupe comme Total et qui semblent particulièrement pertinents.

La sécurité des systèmes d'information dans les entreprises

L'exemple de Total

Total a mis en place un **cadre de référence** complet en matière de sécurité des systèmes d'information, une **politique de classification des ressources et de sécurisation** adaptée au niveau de protection requis par chaque type de données, ainsi qu'un **dispositif de pilotage** pour ajuster, arbitrer et améliorer son dispositif.

Total a défini **sept grands principes d'action** :

1. **Maîtriser les accès aux systèmes d'information** afin de limiter les risques d'intrusion et de restreindre les accès aux seules fonctions et informations nécessaires aux activités, et d'être en mesure de justifier les droits d'accès accordés.

2. **Maintenir la disponibilité et l'intégrité des systèmes d'information** afin de préserver la continuité des activités du groupe et préserver les services offerts aux utilisateurs

3. **Organiser la veille et la surveillance**, détecter au plus tôt les comportements inhabituels, les attaques déloyales et les incidents de sécurité, et limiter leurs impacts dans le cadre d'une réponse coordonnée à l'échelle du groupe, des branches et des filiales.

4. **Définir des périmètres de sécurité homogènes** et compatibles avec les enjeux des métiers afin que les informations circulent dans des conditions cohérentes de sécurité et que ces périmètres limitent les risques de propagation d'intrusion et de déni de service global.

5. **Intégrer formellement la sécurité des systèmes d'information dans les projets** afin d'aligner les fonctions de sécurité sur les enjeux des métiers, et privilégier la prévention et être en mesure d'expliquer les choix effectués.

6. **Conserver et protéger les éléments permettant de reconstituer**, a posteriori, les actions sensibles effectuées sur les systèmes d'information en les imputant à leurs auteurs afin de répondre au mieux aux exigences réglementaires, juridiques et de contrôle.

7. **Sensibiliser et former le personnel** afin de limiter les comportements à risque, améliorer la capacité de réaction de chacun et disposer des compétences nécessaires pour implémenter les dispositifs de sécurité.

● ***Six recommandations***

Le rapport Lasbordes concluait sur les six recommandations suivantes :

- **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**, notamment en renforçant l'autorité des structures en charge de la sécurité des systèmes d'information.

Il préconisait également une **réorganisation de la politique interministérielle de la sécurité des systèmes d'information** en séparant les fonctions d'autorité (élaboration de la politique nationale, validation des politiques de chaque ministère), confiées au SGDN, et les fonctions opérationnelles (veille, formation, conseil, inspection, certification, alerte, politique d'achat public) qui s'appuieraient sur les moyens de l'actuelle DCSSI renforcés et regroupés dans une structure nouvelle à statut d'établissement public industriel et commercial.

2. Des efforts réels mais encore modestes

Le constat sévère du rapport Lasbordes ne doit pas occulter les efforts réels réalisés ces dernières années, dans le cadre de moyens certes limités, pour renforcer notre politique de sécurité des systèmes d'information. Nombre d'entre eux résultent du plan gouvernemental lancé en 2004.

● ***Les capacités de veille et de réaction : le rôle du COSSI et des CERT, le plan Piranet***

Depuis le printemps 2005, la DCSSI dispose d'un **centre opérationnel de la sécurité des systèmes d'information (COSSI)** qui fonctionne 24 heures sur 24, 7 jours sur 7. Le COSSI assure une veille permanente sur l'évolution de la menace, sur les vulnérabilités découvertes dans les divers produits informatiques, sur les attaques conduites dans le monde et sur les incidents affectant notamment les systèmes d'information gouvernementaux. En liaison étroite avec les différents centres ministériels, notamment ceux du ministère de l'intérieur et de la défense, et de nombreux centres homologues étrangers, il se tient prêt à donner l'alerte et à proposer les mesures techniques appropriées de prévention ou de protection. Le COSSI dispose d'un effectif de 25 personnes.

Le COSSI intègre en son sein le Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (**CERTA**) qui avait été créé en 1999 et qui constitue son unité technique. Le CERTA assure, pour le compte de l'administration française, les missions d'information sur les

vulnérabilités, d'assistance en cas d'incidents de sécurité et de traitement des alertes et réactions aux attaques informatiques.

Des structures analogues, baptisées **CERT** (*Computer emergency response team*) existent dans de très nombreux pays du monde et agissent au profit du secteur public comme à celui du secteur privé. **La France compte quatre CERT** : le CERTA, dédié au secteur de l'administration ; le CERT-RENATER, établi au profit de la communauté de l'enseignement supérieur et de la recherche ; le CERT-IST (Industrie, services et tertiaire), centre d'alerte et de réaction constitué sous la forme d'une association de la loi de 1901 et destiné aux entreprises françaises qui ont souhaité y adhérer ; enfin le CERT-LEXSI (Laboratoire d'expertise en sécurité informatique) qui est un prestataire de service commercial.

Le **dispositif de réaction** en cas d'attaques de grande ampleur sur les systèmes d'information de l'État et des opérateurs d'infrastructures d'importance vitale repose sur les mesures de sécurité des systèmes d'information insérées dans le plan gouvernemental de vigilance Vigipirate et par la mise sur pied du **plan gouvernemental de réponse aux crises Piranet**.

LE PLAN PIRANET

Le plan Vigipirate permet de se préparer à d'éventuelles attaques informatiques en fonction du niveau perçu de la menace.

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.

Dans la continuité du plan Vigipirate, il vise à permettre aux autorités gouvernementales de réagir rapidement à tout événement grave en mobilisant sans délais tous les acteurs concernés, en prenant les premières décisions imposées par l'urgence et en veillant à la cohérence des actions entreprises par les différents départements ministériels conformément à leurs responsabilités propres.

Le périmètre pris en compte dans le déclenchement du plan Piranet peut couvrir l'ensemble des services (cas d'une agression massive) ou certains services seulement (cas d'une agression ciblée).

Des plans Piranet spécifiques sont déclinés pour chaque ministère.

Le premier plan Piranet a été créé en 2002, peu après les attentats du 11 septembre 2001. Sa rédaction est régulièrement adaptée en fonction de l'évolution de la menace et du retour d'expérience des exercices.

La mise en œuvre des plans Vigipirate et Piranet suppose l'activation de **centres opérationnels ministériels** agissant en coordination avec le COSSI. Le plan de renforcement de la sécurité des systèmes d'information insistait à cet égard sur la nécessité de garantir la disponibilité en toutes circonstances de ressources humaines compétentes et suffisantes pour constituer ces équipes opérationnelles. La montée en puissance du dispositif dans les différents ministères, en cas de renforcement des mesures Vigipirate dans le domaine de la sécurité des systèmes d'information ou d'activation du plan Piranet, est testée lors des exercices interministériels.

● ***Les activités de formation, de conseil, d'audit et d'entraînement***

La DCSSI dispose d'un **Centre de formation à la sécurité des systèmes d'information** destiné à la formation des acteurs publics concernés. Le rapport Lasbordes avait regretté que ces actions ne puissent pas être développées et ouvertes à un public plus large. Au cours de la période récente, le nombre et les thèmes des formations proposées ont très sensiblement augmenté (16 stages différents, répartis tout au long de l'année en 65 sessions de durées variant entre la journée et 5 semaines). Plus de 1 100 agents de l'Etat en ont bénéficié en 2007. Le centre de formation de la DCSSI entretient des liens étroits avec des établissements d'enseignement supérieur et des centres de formation continue afin d'encourager la prise en compte de la sécurité des systèmes d'information à tous les niveaux et de partager les expériences et réflexions respectives. La DCSSI effectue également de nombreuses démonstrations afin, notamment, de sensibiliser les hautes autorités.

Conformément aux recommandations du rapport Lasbordes, un **portail internet gouvernemental consacré à la sécurité informatique** et destiné au grand public comme aux professionnels a été ouvert au mois de février 2008[1]. Il propose des fiches pratiques et des conseils destinés à tous les publics. Des guides de configuration sont proposés aux utilisateurs pour les aider à mettre en pratique les recommandations faites dans les fiches techniques. Il comporte également des actualités et avertit de menaces nouvellement rencontrées qui appellent une action rapide des utilisateurs pour en limiter les effets.

La DCSSI réalise également un **programme d'inspection** qui vise à vérifier le niveau de sécurité de l'ensemble des ministères sur une période de trois ans. **Fin 2008, l'ensemble des ministères auront été inspectés au moins un fois**. Toutes ces inspections comportent un volet tentative d'intrusion. Les rapports réalisés après chaque inspection sont adressés aux directeurs de cabinet des ministères concernés. Il faut noter que les moyens actuels que la DCSSI peut dégager au profit des inspections ne permettent pas de prendre en compte les opérateurs d'importance vitale.

---

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

Enfin, une **politique d'exercices interministériels** en matière de sécurité des systèmes d'information a été mise en place en 2005. Elle prévoit de réaliser **au moins trois exercices par an**, pouvant être transverses aux différents ministères ou spécifiques à l'un d'entre eux. Au printemps 2008, s'est déroulé l'exercice majeur Piranet 08, auquel ont participé tous les ministères, le cabinet du Premier ministre et deux opérateurs de secteurs d'activité d'importance vitale. Les précédents exercices de mise en œuvre du plan Piranet avaient eu lieu en 2003 et en novembre 2005.

● ***Le développement de réseaux d'information protégés et la diffusion de produits sécurisés***

Dans la lignée des orientations du plan de renforcement de la sécurité des systèmes d'information, d'importants progrès ont été réalisés en vue de **sécuriser les moyens de communication gouvernementaux**.

Le réseau interministériel RIMBAUD a été modernisé. Il sera prochainement doté de nouveaux terminaux de « cryptophonie de nouvelle génération ». Pour les communications de données, l'**intranet sécurisé interministériel ISIS** (Intranet sécurisé interministériel pour la synergie gouvernementale) a été inauguré le 27 novembre 2007. Il s'agit du premier réseau interministériel permettant le partage d'informations classifiées au niveau confidentiel-défense. ISIS constitue également un outil de conduite de l'action gouvernementale lors d'une situation d'urgence ou en cas de crise. D'un périmètre encore limité aux instances centrales, son extension aux autorités déconcentrées est à l'étude. Enfin, le système de messagerie électronique MAGDA a été modernisé et son déploiement a été étendu. Il est interconnecté au réseau ISIS. L'ensemble des préfectures seront desservies fin 2008.

Par ailleurs, un effort important est réalisé pour **développer et acquérir des produits de haut niveau de sécurité** (protection d'informations classifiées au niveau secret-défense) destinés aux services gouvernementaux, notamment pour le chiffrement des communications téléphoniques (terminaux téléphoniques chiffrants) et des échanges de données chiffrées sur internet (boîtiers de chiffrement IP). La DCSSI soutient certaines initiatives industrielles dans des domaines tels que les ressources de chiffrement pour poste de travail, les supports externes chiffrants, les chiffreurs IP individuels ou les assistants personnels sécurisés.

Enfin, la DCSSI développe son activité d'**identification de produits de sécurité** à travers plusieurs niveaux de décisions (certification, qualification, agrément, labellisation) correspondant au niveau de sécurité exigé. Elle met à la disposition des utilisateurs, qu'il s'agisse d'administrations ou d'entreprises, des catalogues désormais plus fournis de produits adaptés à leurs besoins.

● ***La protection des opérateurs d'importance vitale***

La **protection contre les attaques informatiques** fait partie intégrante du **dispositif de sécurité des activités d'importance vitale**, tel qu'il a été réformé pat le décret du 23 février 2006.

Dans chaque secteur d'activités essentielles à la vie nationale, une **directive de sécurité** analyse les risques à partir de scénarios fondés sur les analyses de renseignements. Elle énonce des exigences de sécurité traduites en actions de réduction des vulnérabilités et en dispositions pratiques de protection, ventilées en une posture permanente de sécurité et en mesures graduées en fonction de l'intensité conjoncturelle de la menace.

Ces directives prennent en compte la menace d'attaques informatiques. Il en va de même des plans de sécurité et de protection que chaque opérateur concerné devra établir pour se conformer à la directive nationale.

● ***Les perspectives ouvertes par le renforcement de la lutte contre la cybercriminalité***

Le plan de lutte contre la cybercriminalité annoncé au mois de février 2008 par Mme Michèle Alliot-Marie, ministre de l'intérieur, qui en a fait l'une de ses priorités, comporte des dispositions pouvant intéresser les atteintes à la sécurité des systèmes d'information gouvernementaux ou sensibles, même s'il vise essentiellement la délinquance sur l'internet.

Ce plan prévoit, sur le plan national, des adaptations législatives ou réglementaires permettant de **mieux identifier les utilisateurs d'internet**, notamment en matière de conservation des données de connexion, et la possibilité, sous le contrôle de l'autorité judiciaire, de **capter à distance les données numériques** se trouvant sur un ordinateur.

Il propose également, à l'échelle européenne, d'établir des **accords permettant la perquisition informatique à distance** sans qu'il soit nécessaire de demander au préalable l'autorisation du pays hôte du serveur.

B. DES PARTENAIRES ET ALLIÉS MIEUX ORGANISÉS ET MIEUX ÉQUIPÉS

L'un des constats principaux mis en lumière par le rapport Lasbordes était la **disparité des moyens entre les services français en charge de la sécurité des systèmes d'information et leurs équivalents des principaux pays occidentaux**.

Cette situation n'a guère évolué depuis lors, les **110 agents de la DCSSI** devant être comparés aux **450 agents du service britannique et aux 500 agents du service allemand**, soit un rapport d'environ 1 à 5 entre la France et ses deux principaux partenaires européens.

1. Le Royaume-Uni

La *National Security Strategy of the United Kingdom* rendue publique en mars 2008 par le Premier ministre Gordon Brown identifie les attaques sur les systèmes d'information comme une menace pour la sécurité du pays. Le réseau internet est considéré à ce titre comme une infrastructure vitale du Royaume-Uni.

Le Royaume-Uni a adopté en 2003 une stratégie nationale en matière de sécurité de l'information qui met l'accent sur le **partenariat avec le secteur privé**. La coopération entre acteurs publics et privés se matérialise au sein d'une instance spécifique : la *National infrastructure security coordination center*. Celle-ci traite notamment de la sécurité des réseaux et des systèmes informatisés de contrôles industriels. Un centre de veille et d'alerte lui est également rattaché.

En ce qui concerne les acteurs publics de la sécurité des systèmes d'information, le service homologue de la DCSSI française est le ***Communications and electronic security group (CESG)*** qui compte environ **450 agents**. Il relève de l'agence en charge du renseignement technique, le *Communication government head quarter (CGHQ)*.

Les Britanniques ont entrepris une réforme de leur organisation, avec la création du *Centre for the Protection of National Infrastructure (CPNI)* rattaché au directeur général du *Security Service* (ex *MI5*), chargé notamment de la protection des infrastructures nationales, et du *GocCertUK*, centre opérationnel chargé de la réponse aux attaques informatiques.

Le Royaume-Uni a mis en place un réseau de communication gouvernemental (*GSI - Government secure internet*) qui dispose de passerelles vers l'internet sécurisées.

2. L'Allemagne

L'Allemagne a elle aussi adopté en 2005 un **plan national pour la protection des infrastructures d'information** qui concerne tant le secteur public que le secteur privé.

Sa mise en œuvre s'appuie sur l'agence homologue de la DCSSI, le *Bundesamt für Sicherheit in des Informationstechnik (BSI)*, rattaché au ministère de l'intérieur. Le BSI dispose de compétences assez comparables à celles de la DCSSI (sensibilisation, analyse des risques, veille et alerte, développement de produits de sécurité, normalisation). Il entretient cependant des liens beaucoup plus étroits avec les opérateurs d'infrastructures critiques et les entreprises sensibles.

Le BSI bénéficie d'une **augmentation régulière de ses effectifs**, qui s'élevaient à 340 agents en 2001 et atteignent actuellement **500 agents**.

Il faut aussi souligner qu'à la suite de la réunification et du transfert de la capitale à Berlin, l'Allemagne s'est dotée **de systèmes de communication gouvernementaux extrêmement fiables et hautement sécurisés** (*Informationverbund Berlin Bonn – IVBB*). Cette caractéristique a facilité le déploiement d'outils automatiques de surveillance des réseaux informatiques gouvernementaux qui permettent à l'Allemagne de disposer d'une **capacité de détection** dont la France est encore privée.

3. Les Etats-Unis

Les Etats-Unis accordent de longue date une priorité stratégique à la protection des systèmes d'information.

En mai 1998, le président Clinton signait le décret présidentiel 63 sur la protection de l'infrastructure critique visant à notamment éliminer les vulnérabilités de leurs systèmes informatiques au regard d'attaques cybernétiques comme physiques.

Le *Department of Homeland Security*, 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 réseaux de communication.

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) et offensives (écoute et intrusion) dans le domaine des systèmes d'information. L'*Information assurance directorate*, qui constitue au sein de la NSA le service homologue de la DCSSI, compte environ **3 000 agents**.

Les Etats-Unis procèdent à un **renforcement de leur organisation et de leurs moyens**. Le 8 janvier 2008, le président 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. Cette directive est classifiée mais plusieurs mesures ont été rendues publiques. Parmi celles-ci on peut retenir :

- la montée en puissance du **centre gouvernemental de veille et d'alerte** dont la mission est la protection des infrastructures américaines sur internet ;

- 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** ;

- la création d'un *National Cyber security Center* regroupant les différents services compétents en la matière au sein du *Departement of Homeland Security*.

- l'extension de la *National Cyber Investigative Joint Task Force* au sein du *FBI* avec un **renforcement des capacités de plus de 200 personnes** ;

- 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 États-Unis.

L'ensemble de **ce programme est estimé pour 2009 à 7,2 milliards de dollars**, soit un effort supplémentaire de 600 millions de dollars, et témoigne de l'importance accordée à la protection des réseaux informatiques.

On notera aussi que les Etats-Unis consacrent des moyens conséquents à la réalisation de simulations et d'exercices. Au mois de février 2008, le *Departement of Homeland Security* a réalisé un exercice de grande ampleur baptisé « *CyberStorm II* » 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), cet exercice était doté d'un budget supérieur à 6 millions de dollars). Ses conclusions seront rendues publiques en septembre prochain.

Enfin, on sait que l'**armée américaine** est dotée d'une **doctrine intégrant la lutte informatique défensive** comme la **lutte informatique offensive**. L'annonce par l'*US Air Force* en septembre 2007 de la création d'un « cyber-commandement » en a fourni l'illustration, mais la coordination des capacités dispersées dans les différentes armées ne semble pas encore être optimale.

C. UNE AMORCE DE COOPÉRATION INTERNATIONALE

Les attaques informatiques 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.

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

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

L'Union internationale des télécommunications (UIT) 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 vient de créer 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,

L'OCDE et le G8 mènent également des travaux sur le sujet.

Votre rapporteur évoquera plus précisément les coopérations opérationnelles entre structures d'alerte et d'assistance, ainsi que les actions menées dans le cadre de l'OTAN et de l'Union européenne.

1. La coopération opérationnelle des structures d'alerte et d'assistance (CERT)

Comme on l'a précédemment indiqué, un très grand nombre de pays ont mis en place des CERT (*Computer emergency response team*), structures permanentes d'alerte et d'assistance 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.

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 200 CERT répartis de par le monde**.

Une **enceinte spécifique,** l'**EGC** (*European Government Computer Security Incident Response Teams*), a été créée par **certains pays européens** pour regrouper 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.

D'après les indications de l'Agence européenne de la sécurité des réseaux et de l'information (ENISA), seuls huit pays membres de l'Union européenne disposaient d'un CERT gouvernemental en 2005. Leur nombre s'élève à 14 actuellement et la quasi-totalité des pays membres devraient être dotés d'un CERT gouvernemental d'ici un à deux ans.

2. Une nouvelle priorité de l'OTAN

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 (*Nato computer incident response capability – NCIRC*).

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.

Les réflexions menées depuis lors ont abouti à l'élaboration d'un **concept de cyberdéfense de l'OTAN** qui a été approuvé en début d'année 2008. Lors du sommet de Bucarest, au mois d'avril dernier, les chefs d'Etat et de gouvernement 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* ».

Cette politique de cyberdéfense vise tout d'abord à **renforcer la sécurité des systèmes d'information de l'Alliance**, grâce à l'amélioration des normes et des procédures de sécurité, et à une gestion plus centralisée.

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 à partager.

L'OTAN prévoit de créer une **autorité chargée de la cyberdéfense** (*NATO Cyber Defense Management Authority – CDMA*) qui constituera le point central pour la coordination de la politique de l'Alliance et l'analyse des besoins, en regroupant l'ensemble des compétences en la matière.

Par ailleurs, huit pays alliés[1] ont décidé de contribuer à la création d'un **centre d'excellence sur la cyberdéfense** rattaché à l'OTAN. Constitué à partir d'une capacité estonienne déjà existante, ce centre situé à Tallin et inauguré à la fin du mois de mai dernier est constitué d'une trentaine d'experts provenant des pays impliqués. Ce centre n'a pas de vocation opérationnelle. 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.

Il faut noter que la France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN qui, en moins d'un an, aura permis de définir un concept global et de le décliner en une organisation cohérente.

3. L'action encore lacunaire de l'Union européenne

Les instances européennes ont adopté de **nombreux documents d'orientation et programmes** intéressant directement ou indirectement la sécurité des systèmes d'information. Pour la période récente, on peut citer : 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 propose notamment une évaluation comparative des politiques nationales relatives à la sécurité des réseaux et de l'information ; la communication de la Commission du 12 décembre 2006 sur un programme européen de protection des infrastructures critiques qui préconise une approche européenne commune de la sécurité de ces infrastructures et inclura nécessairement les préoccupations liées aux systèmes d'information.

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

L'Union européenne dispose cependant d'un instrument spécialisé à travers l'Agence européenne chargée de la sécurité des réseaux et de

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

l'information, l'**ENISA** (*European Network and Information Security Agency*), 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** : conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle ; recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents ; promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité de faire face aux menaces pesant sur la sécurité de l'information ; favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées; suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

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.

Une proposition de règlement prévoit la prolongation à l'identique du mandat de l'ENISA jusqu'en 2011, date à laquelle son avenir devrait être réexaminé.

Cette perspective de réorganisation témoigne des **interrogations qui subsistent sur les missions et l'action de l'ENISA** au service des objectifs poursuivis par l'Union européenne.

Le Livre blanc sur la défense et la sécurité nationale rendu public le 17 juin dernier souligne à cet égard que « *l'efficacité de l'agence européenne ENISA devra également 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.

Par ailleurs, le Livre blanc juge **indispensable de renforcer la coopération opérationnelle** au sein de l'Union européenne, afin qu'elle soit la plus réactive possible entre Etats membres face aux attaques contre les systèmes d'information.

La France proposera également que la **Commission impose aux opérateurs des règles de durcissement des réseaux et des procédures** destinées à en accroître très fortement la résilience.

III. LA NÉCESSITÉ D'UNE IMPULSION POLITIQUE FORTE ET DE MOYENS RENFORCÉS

En dépit des actions positives entreprises au cours des dernières années, amplifiées après l'adoption du plan interministériel de 2004, la situation de la France au regard de la menace provenant des attaques informatiques reste insatisfaisante.

Nous ne disposons **pas de véritable capacité de surveillance et de détection des attaques informatiques**.

L'échelon interministériel ne dispose **pas 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.

Les textes ne lui donnent **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.

A fortiori, **la synergie entre acteurs publics et privés reste insuffisante** alors qu'un partenariat étroit serait indispensable.

Dans ce contexte, la place accordée à la cyberdéfense par le **Livre blanc sur la défense et la sécurité nationale** doit être saluée. Elle témoigne d'une prise de conscience renforcée de la menace. Elle est porteuse de beaucoup d'espoirs en termes d'amélioration de notre organisation et de renforcement de nos moyens.

Votre rapporteur considère que **les orientations fixées par le Livre blanc constituent une base solide pour rattraper le retard accumulé** ces dernières années par notre pays en la matière. Il souhaite cependant qu'elles soient rapidement assorties des décisions qui permettront de **les traduire dans les faits** et il effectuera, dans cette perspective, plusieurs propositions.

A. UNE PRIORITÉ RECONNUE PAR LE LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE

Le Livre blanc sur la défense de 1994 avait brièvement mentionné les menaces pesant sur les systèmes informatiques au titre des vulnérabilités nouvelles à prendre en compte. Le Livre blanc sur la sécurité intérieure face au terrorisme, publié en 2006, avait quant à lui souligné de manière plus précise la nécessité de protéger les systèmes informatiques sensibles, dans la perspective d'actions terroristes visant à désorganiser ou paralyser le fonctionnement du pays.

Avec le Livre blanc de 2008, la **protection des systèmes d'information** est clairement définie comme une **composante à part entière de notre politique de défense et de sécurité**.

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.

Les orientations définies par le Livre blanc en termes d'organisation et de moyens découlent de ce constat.

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

L'une des principales décisions arrêtées dans le cadre du Livre blanc réside dans 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 sera **constituée à partir de l'actuelle Direction centrale de la sécurité des systèmes d'information (DCSSI)**. Elle relèvera du Premier ministre et sera distincte des services du **SGDN** tout en étant placée sous la **tutelle** de celui-ci, qui deviendra par ailleurs le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

D'après les informations fournies à votre rapporteur, cette agence serait constituée sous le **statut de service à compétence nationale**, qui a été créé pour des structures à vocation opérationnelle et lui confèrerait une certaine autonomie, mais pas de personnalité juridique propre et distincte de celle de l'Etat. On rappellera que le rapport Lasbordes avait suggéré l'institution d'un établissement public industriel et commercial, le SGDN conservant les fonctions d'autorité.

Le Livre blanc évoque les compétences qui seront confiées à l'agence, sans les détailler. Sur le plan opérationnel, elle mettra en œuvre une **capacité centralisée de détection et de défense** face aux attaques informatiques. Elle aura en charge le développement et l'acquisition des **produits de sécurité essentiels à la protection des réseaux les plus**

sensibles. Elle assurera également une **mission de conseil auprès du secteur privé**, notamment dans les secteurs d'activité d'importance vitale. L'agence devra servir de **réservoir de compétences** au profit des administrations et des opérateurs d'infrastructures vitales.

S'agissant des **effectifs** et des **moyens financiers** de la future agence, le Livre blanc indique simplement qu'ils seront **sensiblement renforcés par rapport à ceux de la DCSSI**.

Ce dispositif sera complété par la mise en place d'**observatoires de la sécurité des systèmes d'information dans les zones de défense et de sécurité**. Un réseau territorial d'experts sera ainsi constitué auprès des préfets de zone de défense, avec une mission de soutien en formation et en conseil aux administrations locales, d'animation de réseau et de remontée des signaux précurseurs d'incidents.

2. Le renforcement des capacités de détection et de protection

Le Livre blanc préconise « *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.

Le Livre blanc prévoit ainsi la mise sur pied d'un **centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre des mécanismes de défense adaptés**.

Comme on l'a précédemment précisé, **la France ne dispose pas d'une telle capacité de détection précoce, à la différence de l'Allemagne**, alors que les Etats-Unis viennent pour leur part de décider que le dispositif de détection opérationnel depuis plusieurs années sur les réseaux du Pentagone serait étendu à toute l'administration et aux agences fédérales, ainsi éventuellement qu'aux installations d'importance vitale.

Le centre opérationnel fonctionnant en permanence à la DCSSI (COSSI) se limite à une veille sur la partie visible de l'internet, mais n'a

aucun moyen de surveiller et d'analyser les flux transitant entre l'internet et les administrations.

Votre rapporteur estime que **la mise en place rapide de ce centre de détection est absolument indispensable**. Il précise en outre que la capacité de surveillance dont il disposera portera exclusivement sur les traces informatiques laissées par les flux de données transitant entre les réseaux gouvernementaux et l'extérieur, et non sur le contenu des communications électroniques elles-mêmes. Des outils informatiques spécialisés permettent de collecter ces données et de les analyser pour déceler les signes d'attaques informatiques.

En matière de protection, le Livre blanc prévoit la généralisation du recours à des produits de sécurité et à des réseaux de confiance, ce qui suppose d'une part la **maîtrise industrielle nationale de produits de très haute sécurité** pour la protection des secrets de l'Etat, et d'autre part une offre étendue de produits et services de confiance labellisés.

Enfin, le Livre blanc préconise des mesures réglementaires pour **imposer aux opérateurs de communications électroniques une protection renforcée de leurs réseaux** contre les pannes et les attaques les plus graves. Il estime que le réseau internet doit être considéré comme une infrastructure vitale et que sa résilience doit être améliorée.

3. La nécessité de capacités « offensives »

En présentant le Livre blanc le 17 juin dernier, le Président de la République a 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.

En ce qui concerne la référence aux capacités offensives, il convient de distinguer la compétence générale qui revient aux services de renseignement et la mise en place de capacités spécifiquement militaires.

S'agissant des **services de renseignement**, le Livre blanc prévoit un développement des capacités techniques consacrées au réseau internet, « *devenu crucial pour notre sécurité* ». Le renforcement des moyens techniques devrait s'accompagner d'une augmentation du nombre de techniciens et d'experts spécialisés dans ce domaine.

Votre rapporteur estime également qu'un cadre juridique devra être défini pour autoriser des « perquisitions informatiques » facilitant les investigations sur les agresseurs.

S'agissant des forces armées, le Livre blanc estime nécessaire d'acquérir une **capacité de lutte informatique offensive** destinée à neutraliser les centres d'opérations adverses.

Cette capacité figurait parmi les moyens de commandement, de renseignement et d'appréciation inscrits à notre modèle d'armée[1], mais elle n'a pas été développée à ce jour.

Elle 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, sur la base bien entendu d'un cadre juridique et d'une doctrine d'emploi bien définis :

- 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 ;

- 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.

B. UN EFFORT À ACCENTUER DE MANIÈRE RÉSOLUE

Le Livre blanc marque une inflexion significative par la place qu'il accorde à la protection des systèmes d'information sensibles dans notre politique de défense et de sécurité, mais également par les éléments nouveaux et majeurs qu'il apporte et qui sont de nature à donner une impulsion forte à la prise en compte de la sécurité des systèmes d'information dans notre pays.

Il reste désormais à **faire suivre ces orientations de progrès concrets**, particulièrement nécessaires dans un domaine où la France accuse un réel retard face à une menace qui, elle, évolue très rapidement.

---

[1] *Cf rapport annexé à la loi de programmation militaire pour les années 2003 à 2008 (§2.3.2)*

Votre rapporteur considère qu'il faudra à cet effet agir sur deux leviers : les moyens humains et techniques ; une organisation fonctionnant de manière à rendre effectives les prescriptions édictées en matière de sécurité de systèmes d'information.

Par ailleurs, au-delà de la problématique abordée par le Livre blanc, il estime qu'un effort beaucoup plus important doit être réalisé pour créer un véritable partenariat entre les acteurs publics et le secteur privé autour de la sécurité de systèmes d'information.

1. Porter nos moyens à hauteur de ceux de nos homologues européens

Le Livre blanc précise que la future agence chargée de la sécurité des systèmes d'information reprendra les effectifs et les moyens de la DCSSI « *tout en les renforçant sensiblement* ».

Rappelons une nouvelle fois que ces moyens sont aujourd'hui, de l'avis général, notoirement sous-dimensionnés, et quatre à cinq fois inférieurs à ceux de nos partenaires allemand ou britannique.

On ne peut sur ce point se satisfaire d'un simple renforcement « sensible », et le Livre blanc aurait gagné à indiquer un objectif plus précis et surtout plus 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**.

Les volumes d'effectifs et d'investissements concernés sont au demeurant modestes.

Dans un premier temps, un **plan pluriannuel sur trois ou quatre ans** devrait au moins permettre de passer des 110 agents de la DCSSI à une « masse critique » de l'ordre de 300 agents, et de renforcer parallèlement l'effort d'investissement.

Un tel plan permettrait d'obtenir des améliorations notables et concrètes à des échéances relativement proches, notamment :

- de **mettre sur pied** et d'armer en personnels le **centre de surveillance et de détection** crée au sein de l'agence ;

- 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 ;

- 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 constituer au sein de l'agence le **réservoir de compétences** prévu par le Livre blanc ; il permettrait de regrouper l'expertise en sécurisation des réseaux 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 ;

- 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.

2. Donner plus de force à la politique de la sécurité des systèmes d'information

La création d'une agence autonome, dans le cadre du statut de service à compétence nationale, est incontestablement de nature à améliorer la visibilité de la structure centrale en charge de la sécurité des systèmes d'information, de lui permettre d'être mieux identifiée comme l'interlocuteur unique par les administrations et les entreprises et donc de donner davantage d'écho à son action.

La simple transformation de la DCSSI en agence ne saurait cependant suffire à remédier aux faiblesses de notre organisation, telles qu'elles avaient été identifiées notamment par le rapport Lasbordes, ni au risque de dispersion qu'il mentionnait.

Le Livre blanc n'apporte pas, de ce point de vue, de réponse claire à la **question de la gouvernance globale des différents acteurs**, de la **coordination de leur action** et de la **mise en synergie de leurs moyens**. Or, aux côtés de la future agence, ces acteurs vont continuer à jouer un rôle important, qu'il s'agisse 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 et le soutien aux entreprises, ou des services de renseignement, qui disposent d'équipements techniques et de personnels spécialisés déjà conséquents et devraient les voir renforcés au cours des prochaines années.

Il semble à votre rapporteur que cette coordination, nécessaire pour veiller à la cohérence des actions et des moyens, doit **relever 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. Il lui semble également qu'un lien devra être établi, par l'intermédiaire du coordinateur du renseignement, avec le **Conseil national du renseignement** dont la création est prévue par le Livre blanc. La protection des systèmes d'information sensibles entrant dans la mission des

services de renseignement qui disposent à cet effet de capacités importantes, les orientations retenues par ce Conseil devront s'intégrer dans la politique globale de sécurité des systèmes d'information.

S'agissant des **prérogatives de l'agence**, elles ne sauraient se traduire par une sorte de tutelle sur la politique informatique des différentes administrations. Pour autant, elles ne devront pas se limiter à de simples recommandations laissées à la libre appréciation des administrations. Ces prérogatives devront être définies de manière suffisamment claire pour permettre une mise en œuvre effective des prescriptions touchant à la sécurité de systèmes d'information.

Aux yeux de votre rapporteur, l'agence devrait ainsi être en mesure :

- d'**imposer aux administrations une réduction du nombre de leurs passerelles vers l'internet**, à l'image de l'architecture du réseau RENATER, afin de faciliter l'action du centre de surveillance et de détection ;

- 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 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 ;

- d'**étendre ses missions d'inspection et la réalisation des tests d'intrusion aux opérateurs d'importance vitale**.

3. Renforcer le partenariat avec le secteur économique

Il ne revenait pas au Livre blanc de traiter de la problématique particulière des entreprises au regard de la sécurité des systèmes d'information. Cette **dimension essentielle devra néanmoins être prise en compte par la nouvelle organisation**. L'institution d'une agence interministérielle, dotée de moyens moins limités que ceux de l'actuelle DCSSI, devrait aussi se traduire, selon votre rapporteur, par un renforcement du partenariat avec le secteur privé, aujourd'hui insuffisamment développé, comme l'avait souligné le rapport Lasbordes.

Les entreprises, votre rapporteur l'a constaté lors de ses auditions, attendent en premier lieu de l'Etat qu'il leur désigne un **interlocuteur unique**, pour répondre à leurs demandes d'expertise, de conseils, d'assistance. L'agence chargée de la sécurité des systèmes d'information semble toute désignée pour jouer ce rôle. De par sa nature interministérielle, elle pourrait réunir des compétences aujourd'hui dispersées dans d'autres structures et disposer d'une cellule capable de diriger les demandes qu'elle ne peut elle-même traiter vers les organismes compétents des administrations.

Deuxièmement, les entreprises les plus concernées par la sécurité des systèmes d'information (opérateurs d'importance vitale, entreprises intervenant dans des domaines sensibles) attendent **des échanges d'information beaucoup plus fournis et des contacts beaucoup plus fréquents avec les services de l'Etat**. Les moyens dont sera dotée l'agence devront lui permettre de développer la communication vers ces entreprises et de mettre en place des enceintes permettant des contacts réguliers.

Le **développement de l'offre de produits labellisés** constitue la troisième grande attente des entreprises. Ce sera un objectif prioritaire pour la future agence.

Le partenariat avec le secteur privé doit également contribuer au **soutien à la base industrielle et technologique** en matière de produits sécurisés, notamment à l'égard des PME-PMI du secteur. Ne pourrait-on pas imaginer que **les grands groupes s'associent**, par exemple au travers d'un groupement d'intérêt économique, **pour mutualiser leurs besoins en produits sécurisés** et soutenir leur développement par le tissu industriel national ou européen ? Cette politique commune des entreprises pourrait être coordonnée avec celle de l'Etat dans les domaines où les besoins sont communs.

Enfin, le **financement public de la recherche-développement** en matière de sécurité des systèmes d'information doit être accentué. 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. Ce **dispositif doit 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

CONCLUSION

Bien que leurs conséquences se soient avérées relativement limitées, les évènements survenus en Europe ces derniers mois ont clairement montré la réalité de la menace liée aux attaques informatiques.

L'existence de groupes de pirates informatiques qui monnayent leurs savoir-faire, la diffusion de technologies toujours plus sophistiquées exploitant les vulnérabilités des systèmes d'information et la constitution de capacités offensives par les Etats laissent à penser que les actions de ce type se poursuivront et s'amplifieront, car elles offrent un moyen discret et relativement peu coûteux de pénaliser ou de fragiliser un pays.

L'une des caractéristiques de cette menace est son évolution très rapide, puisqu'elle s'adapte en permanence aux derniers développements de la technologie.

Dès lors, il devient on ne peut plus urgent pour la France de rattraper dans ce domaine un retard identifié depuis plusieurs années.

Le Livre blanc sur la défense et la sécurité nationale en offre l'opportunité, car jamais auparavant un document de nature stratégique n'avait effectué une analyse aussi précise de la menace, ni conclu que les moyens d'y faire face faisaient partie intégrante de notre politique de défense et de sécurité.

En prévoyant la création d'une agence interministérielle chargée de la sécurité des systèmes d'information, l'acquisition d'une capacité centralisée et permanente de surveillance et de détection des attaques informatiques, ainsi que le développement de capacités de lutte informatique offensive, le Livre blanc pose les bases d'un indispensable renforcement des réponses, aujourd'hui très insuffisantes, que nous apportons à une réalité déjà inquiétante.

Il importe désormais de traduire ces orientations par des progrès rapides et concrets.

Aux yeux de votre rapporteur, la mise en place d'une nouvelle agence ne sera utile que si celle-ci se voit réellement dotée d'une réelle autorité sur les enjeux les plus critiques de la sécurité des systèmes d'information gouvernementaux, et si elle s'accompagne d'un renforcement de la coordination interministérielle actuellement insuffisante.

D'autre part, le renforcement des moyens est indispensable et urgent. Leur niveau actuel, cinq fois inférieur à celui de nos partenaires principaux, ne permet déjà pas aux structures existantes de faire face dans des conditions satisfaisantes aux missions qui leur ont été confiées. L'accentuation résolue des moyens est a fortiori impérative dès lors que la future agence exercera des compétences élargies.

Les enjeux en termes d'effectifs et d'investissements sont extrêmement modestes au regard des masses financières du budget de l'Etat. Un plan pluriannuel devrait permettre d'ici trois ou quatre ans de disposer de moyens beaucoup plus significatifs, l'objectif devant être, à moyen terme, d'arriver à un niveau équivalent avec celui de pays tels que l'Allemagne ou le Royaume-Uni.

C'est à cette condition que notre dispositif public pourra réellement jouer tout son rôle en matière de sensibilisation, de formation, de renforcement de la protection, de vérification, de surveillance et de réponse aux menaces, au service de l'Etat tout d'abord, mais aussi plus largement de l'ensemble des organismes publics ou privés dont la protection intéresse notre défense et notre sécurité.

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 8 juillet 2008.

A la suite de l'exposé du rapporteur, M. Josselin de Rohan, président, a souligné l'ampleur des défis à relever pour renforcer la protection de nos systèmes d'information face aux attaques informatiques. Il a rappelé que les pays de l'OTAN avaient pris en compte cette menace en adoptant cette année le concept de cyberdéfense de l'Alliance et en créant un centre d'expertise à Tallin, en Estonie.

Appuyant le rapporteur, M. Josselin de Rohan, président, a insisté sur la nécessité de prolonger rapidement les orientations définies par le Livre blanc au travers de mesures concrètes visant à accentuer la politique de sécurité des systèmes d'information et les moyens qui lui sont consacrés. Il a jugé indispensable de porter ces moyens à la hauteur de ceux de nos partenaires européens. Par ailleurs, évoquant les restructurations à venir au ministère de la défense, il s'est demandé si des spécialistes des armées dans le domaine des systèmes d'information et de communication ne pourraient pas être redéployés vers la future agence chargée de la sécurité des systèmes d'information.

M. Robert Hue a estimé qu'il était du devoir de l'Etat de renforcer rapidement notre dispositif de protection face aux attaques informatiques, ainsi que l'avait souligné le rapporteur. Il s'est interrogé sur les incidences budgétaires d'un tel renforcement. Par ailleurs, il s'est félicité de constater que des entreprises publiques comme EDF avaient pris les dispositions nécessaires en matière de sécurité informatique, ce qui démontrait que de telles mesures étaient techniquement accessibles, même si elles ne sont pas généralisées au sein de l'Etat et du monde de l'entreprise.

M. Philippe Nogrix a demandé si les pays européens coordonnaient leurs efforts face à la menace informatique.

M. Jean-Pierre Fourcade a indiqué que la volonté de renforcer les moyens humains en matière de sécurité des systèmes d'information risquait de se heurter à la difficulté de recruter au profit de l'Etat certaines spécialités très recherchées, notamment des mathématiciens de haut niveau. Il a estimé qu'une action devait être menée en amont au profit des filières de formation concernées. Par ailleurs, il a approuvé les remarques du rapporteur s'agissant de la dispersion des différents acteurs impliqués dans la sécurité des systèmes d'information, en souhaitant une coordination plus efficace, sans superposition de structures inutiles.

A la suite de ces interventions, M. Roger Romani, rapporteur, a apporté les précisions suivantes :

- la direction centrale de la sécurité des systèmes d'information dispose aujourd'hui de personnels de grande qualité, mais en nombre très insuffisant ;

- l'affectation de techniciens des armées concernés par les restructurations à venir pourrait effectivement être utilement envisagée pour répondre aux besoins de l'agence chargée de la sécurité des systèmes d'information ; celle-ci aura également besoin de pouvoir recruter de jeunes diplômés sur des contrats à durée déterminée leur permettant ultérieurement de rejoindre, s'ils le souhaitent, le secteur privé ;

- l'impact financier d'un renforcement des moyens humains serait modeste, puisqu'il s'agirait d'ici trois ou quatre ans de porter les effectifs de l'actuelle direction centrale de la sécurité des systèmes d'information de 100 à environ 300 agents, avec à moyen terme l'objectif d'atteindre un niveau proche de celui des Allemands ou des Britanniques, qui disposent d'environ 500 agents dans leurs services équivalents ;

- les autorités européennes ont pris conscience des enjeux de la sécurité des systèmes d'information mais n'ont pas mis en place pour l'instant de structure permettant d'apporter une véritable réponse commune ;

- la coordination interministérielle des différents intervenants doit être améliorée afin d'assurer une meilleure synergie des actions et des moyens.

ANNEXE I -

LISTE DES PERSONNES AUDITIONNÉES

● Personnalités qualifiées

M. Pierre LASBORDES, Député de l'Essonne

M. Jean-Michel HUBERT, Président délégué du comité stratégique pour le numérique auprès du Premier ministre

● Secrétariat général de la défense nationale

M. Francis DELON, Secrétaire général de la défense nationale

M. Patrick PAILLOUX, Directeur central de la sécurité des systèmes d'information

M. Alain JUILLET, Haut-responsable pour l'intelligence économique

● Ministère de la défense

Vice-amiral d'escadre Xavier PAÏTARD, Chef du cabinet militaire du ministre de la défense

M. Henri SERRES, Directeur général des systèmes d'information et de communication

Colonel Didier LOOTEN, Fonctionnaire de sécurité des systèmes d'information

M. Bernard BARBIER, Directeur technique, Direction générale de la sécurité extérieure

M. Eric WARINGHEM, Directeur-adjoint du Centre interarmées de concepts, de doctrines et d'expérimentation

● Ministère de l'intérieur

M. Michel PAGÈS, Sous-directeur des technologies du renseignement, Direction centrale du renseignement intérieur

● Entreprises

- Aéroports de Paris :

M. Jean-Louis BLANCHOU, Directeur de la sûreté

Mme Claire BOTHEREL, Responsable Sécurité des Systèmes d'Information

M. Thierry FEYBESSE, Directeur de l'informatique

Mme Stéphanie ARNOUX-COUDERC, Chargée des relations avec le Parlement

- Total :

M. Patrick HERENG, Directeur des systèmes d'information et des télécommunications

M. Jacques THARALDSEN, Directeur de la sûreté

M. Christophe CEVASCO, Chargé des relations avec le Parlement

- EDF :

M. Jean-Marc SABATHÉ, Directeur de la sécurité

M. Renaud de BARBUAT, Directeur des systèmes d'information

M. Bertrand LE THIEC, Chargé des relations avec le Parlement

ANNEXE II - GLOSSAIRE

1. Termes techniques

botnet : un *botnet*, autrement dit un « réseau de robots », est un réseau de machines compromises 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.

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.

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 ou les vers sont deux 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 (***Denial of distributed service***) : voir déni de service distribué.

DoS (***Denial of service***) : voir déni de service.

enregistreur de frappe (*keylogger*) : logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au 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.

malware : voir code malveillant.

outil de dissimulation d'activité (*rootkit*) : tout programme ou ensemble de programmes 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 outil permettant de protéger un ordinateur connecté 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.

rootkit : voir outil de dissimulation d'activité.

spam : voir pourriel.

spyware : voir logiciel espion.

zombie : machine compromise incluse dans un réseau (botnet) contrôlé par un individu malveillant.

2. Sigles et abréviations

AQSSI : autorité qualifiée en sécurité des systèmes d'information

BSI : *Bundesamt für Sicherheit in des Informationstechnik* (service homologue de la DCSSI en Allemagne)

CALID : Centre d'analyse de lutte informatique défensive (ministère de la défense)

CDMA : *NATO Cyber Defense Management Authority* (OTAN)

CELAR : Centre électronique de l'armement (ministère de la défense – délégation générale pour l'armement)

CERT – Computer emergency response team (équipe de réponse aux attaques informatiques)

CERTA : Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (secrétariat général de la défense nationale – direction centrale de la sécurité des systèmes d'information)

CESG : *Communications and electronic security group* (service homologue de la DCSSI au Royaume-Uni)

COSSI : Centre opérationnel de la sécurité des systèmes d'information (secrétariat général de la défense nationale – direction centrale de la sécurité des systèmes d'information)

DCSSI : Direction centrale de la sécurité des systèmes d'information (secrétariat général de la défense nationale)

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)

OPVAR : organisation permanente veille, alerte, réponse

RENATER : réseau national de télécommunications pour la technologie, l'enseignement et la recherche (groupement d'intérêt public fédérant les infrastructures de télécommunications pour l'enseignement et la recherche)

SCADA : *Supervisory, control and data acquisition* (systèmes de supervision et de régulation)