NOTE DE SYNTHÈSE

RÉPUBLIQUE FRANÇAISE

SÉNAT

CYBERDÉFENSE : UN NOUVEL ENJEU DE SÉCURITÉ NATIONALE

Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat

Rapport d'information n° 449 (2007-2008)

de M. Roger ROMANI

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

1. Une menace aux manifestations de plus en plus évidentes

La paralysie qui a affecté durant plusieurs semaines, au printemps 2007, les sites du gouvernement, des banques et des opérateurs téléphoniques en **Estonie**, puis l'annonce des **tentatives d'intrusion informatiques en provenance de Chine** ciblant des diplomates français et divers services occidentaux, ont matérialisé la réalité d'attaques informatiques dont la nature et les formes étaient encore mal perçues en Europe.

Les **attaques par déni de service**, qui visent à saturer un système informatique par des dizaines ou des centaines de milliers de connexions simultanées, s'appuient sur des réseaux d'ordinateurs contaminés passés à l'insu de leurs propriétaires sous le contrôle de pirates informatiques. Elles peuvent entraîner de fortes perturbations dans la vie économique et sociale d'un pays en interrompant des services en lignes utilisés par les citoyens, les consommateurs et les entreprises. Elles représentent également une menace pour des systèmes opérationnels gérant des services essentiels (distribution d'eau et d'électricité, transports) ou des processus industriels, dès lors qu'ils utilisent des systèmes informatiques de plus en plus connectés au monde extérieur.

Les **intrusions informatiques** utilisent pour leur part des courriers électroniques apparemment légitimes, assorties de pièces jointes piégées permettant de récupérer, par envois fractionnés et discrets, tout le contenu de l'ordinateur.

Ces méthodes ne sont plus le fait d'individus isolés agissant par jeu ou par défi, mais de **groupes organisés de pirates informatiques** professionnels offrant leurs services à la criminalité organisée, à des officines d'espionnage économique, voire à des services de renseignement. Certains Etats se dotent en outre de leurs propres moyens offensifs pour pouvoir mener de telles attaques.

2. Une menace qui ne peut aller qu'en s'accentuant

La place croissante prise par les systèmes d'information et l'internet dans tous les domaines de la vie et du fonctionnement de nos sociétés, l'ouverture et l'interconnexion des réseaux, de même que la généralisation de produits standards dont les vulnérabilités sont en permanence scrutées par les communautés de pirates informatiques, laissent à penser que la

JUILLET 2008

menace informatique ne peut qu'aller en s'accentuant.

Ce **mode opératoire** est **relativement accessible** et **peu coûteux**. Il s'affranchit des distances et des frontières. L'**identification des agresseurs** s'avère en outre très difficile, l'utilisation d'une succession d'adresses relais permettant de cacher ou de déguiser leur 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, le lien entre les pirates informatiques et leurs commanditaires étant en outre le plus souvent impossible à établir avec certitude.

II - LA FRANCE EST ENCORE INSUFFISAMMENT PRÉPARÉE ET ORGANISÉE

1. Une prise de conscience récente

Les faiblesses de la France face à la menace d'attaques informatiques avaient été identifiées lors du lancement du **plan gouvernemental de renforcement de la sécurité des systèmes d'information de l'Etat,** en mars 2004, ainsi que dans le **rapport au Premier ministre** publié en janvier 2006 par le **député Pierre Lasbordes**, qui concluait que la France accusait 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».

Depuis lors, certains progrès ont été accomplis, avec la création d'un centre opérationnel de la sécurité des systèmes d'information (COSSI) qui assure une veille permanente sur internet, l'élaboration d'un plan Piranet de réponse aux attaques informatiques ou le développement de réseaux de communication gouvernementaux protégés, comme l'intranet interministériel sécurisé (ISIS).

2. Des lacunes persistantes

Notre organisation reste cependant marquée par la **dispersion des différents acteurs** en charge de la sécurité des systèmes d'information et par la très large autonomie des administrations pour la mise en œuvre de leur politique de sécurité, du fait du caractère non contraignant des recommandations édictées en la matière.

Le service pivot, au niveau interministériel, pour la sécurité des systèmes d'information, la direction centrale de la sécurité des systèmes d'information (DCSSI), compte un **effectif réduit** à 110 agents contre 450 pour son homologue britannique et 500 pour son équivalent allemand. Cet effectif est **insuffisant par rapport aux missions très vastes** qui lui sont confiées en matière de sensibilisation, de conseil, d'évaluation, de surveillance et de qualification de produits sécurisés.

La France ne possède pas, à la différence de l'Allemagne, une **capacité centralisée de surveillance et de détection** des flux de données transitant entre les administrations et l'internet.

Enfin, l'**action des pouvoirs publics en direction du secteur privé** en matière de sensibilisation et de conseil n'est pas assez développée. A certaines exceptions près, les entreprises françaises, notamment les PME, paraissent insuffisamment armées face à la menace informatique.

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

1. Une priorité reconnue par le Livre blanc sur la défense et la sécurité nationale

Le Livre blanc estime que le niveau 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**.

Il prévoit de réer, à partir de l'actuelle DCSSI, une **agence chargée de la sécurité des systèmes d'information**. Elle aura en charge le développement et l'acquisition des produits de sécurité essentiels à la protection des réseaux les plus sensibles. Elle assurera une mission de conseil auprès du secteur privé, notamment dans les secteurs d'activité d'importance vitale. Elle servira de réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales.

La future agence mettra en œuvre une **capacité centralisée de détection et de défense face aux attaques informatiques**, à travers un centre assurant une surveillance permanente des réseaux sensibles et doté d'outils spécialisés permettent d'analyser les flux de données pour déceler les signes d'attaques informatiques.

Enfin, le Livre blanc prévoit le **renforcement de capacités offensives** permettant d'identifier l'adversaire, de mettre à jour son mode opératoire, de le neutraliser, voire de lui appliquer des mesures de rétorsion. Elles reposeront sur les services de renseignement, qui verront leurs moyens humains et techniques renforcés à cet effet. Une capacité de lutte offensive spécifiquement militaire sera également développée, compte tenu de la probabilité de voir utiliser l'arme informatique dans les conflits armés.

2. Un effort à accentuer de manière résolue

Les orientations définies par le Livre blanc doivent désormais être rapidement suivies de mesures concrètes.

Il est tout d'abord nécessaire de **porter nos moyens à hauteur de ceux de nos homologues européens**. Alors que le Livre blanc ne mentionne qu'un renforcement « sensible » des effectifs de l'actuelle DCSSI, c'est à une augmentation résolue qu'il faut procéder. L'objectif à se fixer pour le moyen terme doit être de parvenir progressivement, sur plusieurs années, à un niveau similaire à celui des services équivalents de l'Allemagne et du Royaume-Uni. Dans un premier temps, un **plan pluriannuel sur trois ou quatre ans** devrait au moins permettre de passer des 110 agents actuels 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 en matière de capacités de surveillance, de labellisation de produits et services sécurisés, de conseil, d'inspection et d'audit, de communication vers les administrations, les entreprises et le grand public.

Pour **donner plus de force à la politique de la sécurité des systèmes d'information**, la coordination des différents acteurs et la mise en synergie de leurs moyens devront être renforcées sous l'autorité du Premier ministre. Sans s'ériger en tutelle informatique de tous les ministères, la future agence devra exercer un rôle beaucoup plus directif que l'actuelle DCSSI. Elle devra par exemple

pouvoir imposer une réduction du nombre de passerelles entre les ministères et l'internet, pour mieux les surveiller et les sécurisés. Elle devra aussi pouvoir rendre obligatoires certains types de produits sécurisés pour les réseaux les plus critiques, ou s'assurer, pour les autres réseaux sensibles, que les administrations font usage de produits labellisés.

Enfin, **le partenariat avec le secteur économique devra être notablement renforcé**. Les moyens de la future agence devront lui permettre de répondre aux attentes des entreprises qui souhaitent un interlocuteur unique capable de les conseiller, des catalogues plus étoffés de produits labellisés, des échanges d'information et des contacts beaucoup plus fréquents. L'Etat et certaines entreprises sensibles devraient identifier leurs besoins communs ou proches, afin de faire développer par des entreprises françaises, les produits de sécurité très spécifiques qui leur sont nécessaires.

Le présent document et le rapport complet n° 449 (2007-2008)
sont disponibles sur internet :
www.senat.fr/noticerap/2007/r07-449-notice.html

Le rapport peut également être commandé auprès de l'Espace Librairie du Sénat :
Tél : 01.42.34.21.21 - Courriel : *espace-librairie@senat.fr* - Adresse : 20, rue de Vaugirard - 75291 Paris Cedex 06