NOTE DE SYNTHÈSE

RÉPUBLIQUE FRANÇAISE

LA CYBERDÉFENSE : UN ENJEU MONDIAL, UNE PRIORITÉ NATIONALE

Commission des affaires étrangères, de la défense et des forces armées

Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, sénateur du Haut-Rhin

Attaque informatique d'envergure de **Bercy** à la veille de la présidence française du G8 et du G20, espionnage informatique des entreprises à l'image d'**AREVA**, perturbations de sites Internet institutionnels comme celui du **Sénat** : les **attaques contre les systèmes d'information** se sont **multipliées en France**, comme partout dans le monde, ces dernières années. Même **l'Elysée** aurait été récemment victime d'une ou de plusieurs attaque(s) informatique(s).

Par ailleurs, les révélations sur l'implication probable des Etats-Unis dans la conception du virus **STUXNET**, qui a détruit environ un millier de centrifugeuses d'enrichissement de l'uranium, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran, ou encore la récente découverte du virus **FLAME**, vingt fois plus puissant, laissent présager de nouvelles *« armes informatiques »*, aux potentialités encore largement ignorées.

Avec le développement de l'Internet, et leur interconnexion croissante, les systèmes d'information sont désormais les véritables « centres nerveux » de nos sociétés, sans lesquels elles ne pourraient plus fonctionner.

Dans ce contexte, **la France est-elle suffisamment organisée et préparée pour faire face à une attaque informatique ?**

Les attaques contre les systèmes d'information : une menace stratégique qui s'est concrétisée et accentuée ces dernières années

De Tallin à Téhéran : aucun pays n'est aujourd'hui à l'abri des attaques informatiques

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, il ne se passe pratiquement pas une semaine sans que l'on annonce, quelque part dans le monde, **une attaque informatique importante** contre une grande institution publique ou privée.

La France n'est pas épargnée par ce fléau

En France, les administrations, les entreprises ou les opérateurs d'importance vitale (énergie, transports, santé, etc.) sont victimes **chaque jour** de **plusieurs millions** d'attaques informatiques.

Qu'il s'agisse d'« attaques par déni de service » visant à saturer par un nombre élevé de requêtes et à rendre inaccessible un site Internet ouvert au public, à l'image du site du Sénat, de tentatives de pénétration dans les systèmes à des fins d'espionnage, grâce notamment à des « logiciels espions » introduits par un « cheval de Troie », à l'image de l'attaque de Bercy ou d'AREVA, ou encore de véritables « bombes informatiques » visant à détruire les données contenues dans les systèmes d'information, comme STUXNET, **la menace est concrète et protéiforme.**

Ces attaques informatiques peuvent être menées par des pirates informatiques, des groupes d'activistes, des organisations criminelles, mais aussi par des entreprises concurrentes, voire par d'autres Etats. Les soupçons se portent souvent vers la Chine ou la Russie même s'il est très difficile d'identifier précisément les auteurs de ces attaques.

Certes, il ne s'agit pas de prétendre à une protection absolue. Ce serait assez illusoire. Le propre des attaques informatiques est d'exploiter les failles, de se porter là où les parades n'ont pas encore été mises en place. Mais on peut **renforcer la sécurité des réseaux et des infrastructures les plus sensibles** et améliorer **leur résilience**.

18 JUILLET 2012

Une menace désormais prise en compte au niveau international

1. Des alliés mieux armés

- **Les Etats-Unis**

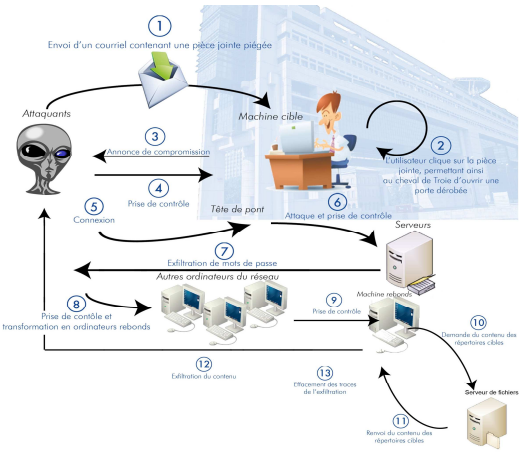
Le Président Barack Obama s'est fortement engagé sur le sujet et a qualifié la cybersécurité de **priorité stratégique**. Il existe plusieurs organismes, au sein du département chargé de la sécurité intérieure ou du Pentagone, qui interviennent dans ce domaine, comme l'Agence de sécurité nationale (NSA) ou le *Cybercommand*. De 2010 à 2015, les Etats-Unis devraient consacrer **50 milliards de dollars** à la cyberdéfense et **plusieurs dizaines de milliers d'agents** travaillent sur ce sujet.

- **Le Royaume-Uni**

Le gouvernement a adopté en novembre 2011 une nouvelle stratégie. Le principal organisme en charge est le *Government Communications Headquarters* (GCHQ), l'agence chargée du renseignement technique. Environ **700 agents** s'occupent des questions de cyberdéfense. Malgré le contexte budgétaire, le Premier ministre David Cameron a annoncé en 2010 un effort supplémentaire de 650 millions de livres (**750 millions d'euros**) sur les quatre prochaines années pour la cyberdéfense.

- **L'Allemagne**

Une stratégie a été élaborée en février 2011. La coordination en incombe au ministère fédéral de l'Intérieur auquel est rattaché l'office fédéral de sécurité des systèmes d'information (BSI) situé à Bonn, qui dispose d'un budget de **80 millions d'euros** et de plus de **500 agents**.



2. Une amorce de coopération internationale

- **L'ONU**

La Chine et la Russie sont les principaux promoteurs d'un traité international et de règles contraignantes dans le cyberespace. Soucieux de préserver la liberté d'expression sur l'Internet, les pays occidentaux s'y opposent et proposent l'élaboration de **mesures de confiance**.

- **L'OTAN**

Depuis le nouveau concept stratégique, adopté lors du Sommet de Lisbonne de 2010, l'OTAN s'est dotée en juin 2011 d'une politique et d'un concept de cyberdéfense. Une autorité de gestion, ainsi qu'un centre d'excellence, situé à Tallin, ont été créés.

Pour autant, **l'OTAN ne paraît pas complètement armée face à cette menace**. La principale unité informatique de l'Alliance n'est pas opérationnelle 24 heures sur 24, 7 jours sur 7. Plus généralement, l'Alliance doit encore déterminer quelle attitude adopter pour répondre à des cyberattaques. **Peut-on invoquer l'article 5 du traité de Washington** ? Il n'existe pas de réponse claire à cette question.

- **L'Union européenne**

L'Union européenne a **un rôle important à jouer** car une grande partie des règles qui régissent les réseaux de communication électroniques relèvent de ses compétences. Toutefois, **la Commission européenne et de nombreux pays membres ne semblent pas encore avoir pris la mesure** des risques et des enjeux liés à la cyberdéfense.

L'emblème de la mouvance Anonymous

Malgré d'importants progrès depuis 2008, notre dispositif connaît encore d'importantes lacunes

1. De réelles avancées depuis 2008

Les rapports Lasbordes de 2006 et Romani de 2008 avaient estimé que la France n'était ni suffisamment organisée ni bien préparée pour faire face à une attaque informatique.
Le **Livre blanc sur la défense et la sécurité nationale de 2008** a identifié la menace et a donné **une réelle impulsion** à la politique de cyberdéfense.

En termes d'organisation, il a permis à cette politique d'être clairement identifiée avec la création, en juillet 2009, de **l'Agence nationale de la sécurité des systèmes d'information** (ANSSI), agence interministérielle qui est l'autorité nationale de défense des systèmes d'information. En février 2011, la France s'est également dotée d'une **stratégie nationale**.

La France dispose, avec cette stratégie et avec l'ANSSI, d'outils importants pour la cyberdéfense. Pour autant, **beaucoup reste à faire dans ce domaine.**

2. Notre dispositif connaît encore d'importantes lacunes

Avec des effectifs de 230 personnes et un budget de 75 millions d'euros, **l'ANSSI reste encore loin des services similaires du Royaume-Uni ou de l'Allemagne**, qui comptent entre 500 et 700 agents.

De plus, si le ministère de la défense et les armées ont pris des mesures, les autres ministères, les entreprises et les opérateurs d'importance vitale restent encore **insuffisamment sensibilisés** à la menace.

Quel serait le moyen le plus simple de provoquer une perturbation majeure de notre pays par le biais d'une attaque informatique ? Un moyen très simple serait de s'en prendre à la distribution d'énergie ou à la santé. L'exemple du virus STUXNET ou celui du ver *Conficker,* qui a perturbé le fonctionnement de plusieurs hôpitaux, montrent que cela n'est pas une hypothèse d'école.

10 priorités et 50 recommandations concrètes pour faire de la protection et de la défense des systèmes d'information une véritable priorité nationale

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

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

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

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

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

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

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

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

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

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

Le logo de l'ANSSI

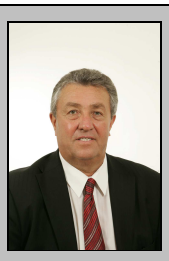
M. Jean-Marie BOCKEL à Washington

Commission des affaires étrangères, de la défense et des forces armées du Sénat :
http://www.senat.fr/commission/etr/index.html

Les rapports de la commission :
http://www.senat.fr/rapports-classes/cretrd.html

Président :

Jean-Louis CARRÈRE



Secrétariat de la commission
15, rue de Vaugirard
75291 Paris Cedex 06

Téléphone : 01.42.34.38.97
Télécopie : 01.42.34.47.63
secretariat-affetra@senat.fr

Rapporteur :

Jean-Marie BOCKEL