Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Centre d'analyse stratégique

Paris, le 19 mars 2013

Présentation de la Note d'analyse

« Cybersécurité : l'urgence d'agir »

Mardi 19 mars 2013

Intervention de Vincent Chriqui,
Directeur général du Centre d'analyse stratégique

Seul le prononcé fait foi

L'actualité récente témoigne de l'intérêt porté à la cybersécurité au niveau international :

- **Aux États-Unis, dans son discours annuel sur l'état de l'Union le 12 février dernier, Barack Obama a annoncé la signature d'un décret visant à renforcer la sécurité des infrastructures critiques contre des cyberattaques**, dans les domaines de l'électricité, de la finance et du transport aérien. Il a aussi encouragé le Congrès à prendre de nouvelles mesures afin de renforcer la sécurité des réseaux et la prévention des attaques ;
- **Quelques jours auparavant, la Commission européenne avait publié son premier plan stratégique de cybersécurité**, visant à maintenir un cyberespace « ouvert, sûr et sécurisé ». Elle a également publié une proposition de directive sur la sécurité des réseaux et de l'information ;

- **En France, le prochain Livre blanc sur la défense et la sécurité nationale**, dont les conclusions devraient être dévoilées prochainement, abordera à n'en pas douter cette question stratégique, comme ce fut le cas en 2008.

Les médias font aussi régulièrement écho de la découverte d'attaques informatiques. **En janvier 2013, les principaux quotidiens américains, parmi lesquels le *New York Times* et le *Wall Street Journal*, ont affirmé avoir été victimes d'espionnage de grande ampleur visant les mots de passe, emails et données de leurs journalistes**. **En février,** ce sont deux des principaux réseaux sociaux, **Twitter et Facebook**, qui ont à leur tour annoncé avoir été touchés par des attaques similaires.

Ces révélations successives d'attaques informatiques traduisent une réalité que le Centre d'analyse stratégique a pu constater au cours d'auditions conduites depuis plusieurs mois auprès des principaux acteurs du domaine : **les attaques informatiques se multiplient, se complexifient et le niveau de la menace auquel sont confrontés organisations et particuliers augmente.**

Trois évolutions marquantes expliquent cette augmentation des attaques informatiques :

- En raison d'interactions croissantes entre les mondes virtuel et réel, **des attaques peuvent toucher des infrastructures physiques. Le désormais célèbre ver Stuxnet, découvert en 2010, avait par exemple pour but de s'attaquer au programme d'armement nucléaire iranien, en sabotant le processus d'enrichissement de l'uranium**. Le niveau de sophistication technique de certaines de ces attaques est tel que seules des puissances étatiques pourraient en être à l'origine. Le développement de l'Internet des objets, qui va connecter des objets de la vie courante à Internet (lunettes, voitures, dispositifs de santé, etc.), va considérablement étendre la menace informatique au monde réel. Je vous laisse imaginer les dégâts que pourrait causer un pirate informatique qui prendrait le contrôle d'une voiture connectée ou d'un *pacemaker* !
- **Deuxième phénomène marquant, on constate un développement préoccupant du « cyberespionnage »,** aussi connu sous le nom d'« *Advanced persistent threats* » (APT). **Ces attaques visent à piller le patrimoine informationnel des organisations :** activité de R&D, données financières et commerciales. Parmi les exemples les plus connus, on pense bien sûr aux **attaques contre le ministère de l'Économie et des Finances en 2010 dans le contexte de la présidence française du G8 et du G20, ou bien encore à l'espionnage dont a été victime l'entreprise Areva pendant plusieurs mois.** La plupart des organisations sont ou ont été victimes d'intrusions informatiques à des fins d'espionnage.
- **L'essor de la cybercriminalité constitue la troisième évolution marquante de ces dernières années** : dirigées contre les entreprises mais surtout contre les particuliers, les attaques sont diffusées massivement dans le but de maximiser les gains financiers. L'hameçonnage ou *phishing* est très utilisé pour soutirer des renseignements personnels (numéro de carte de crédit, mots de passe, etc.) en faisant croire à la victime qu'elle s'adresse à un tiers de confiance (banque,

administration). Les logiciels antivirus classiques sont souvent inefficaces contre ce type d'attaques, les particuliers y sont donc extrêmement vulnérables. La cybercriminalité connait une forte croissance sous l'impulsion du crime organisé, encouragé par un risque pénal relativement faible au regard des montants en jeu.

Ces différentes attaques constituent une véritable menace pour la compétitivité économique et la souveraineté nationale. Le Livre Blanc de 2008 avait consacré la sécurité des systèmes d'information comme l'une des quatre priorités stratégiques pour la France. Cependant, force est de constater que 5 ans plus tard, les organisations sont toujours insuffisamment protégées pour y faire face, **et ce pour deux raisons**.

D'une part**, le degré de sensibilisation au risque informatique est très variable, et souvent faible** au sein des entreprises. Pourtant, la protection des systèmes d'information n'est pas seulement une question technique à confier au DSI, **c'est une question stratégique et organisationnelle**, **qui nécessite une prise de conscience au plus haut niveau.** La sécurité des systèmes d'information est souvent considérée comme un poste de coût à réduire, alors qu'il s'agit d'un investissement sur le long terme destiné à pérenniser l'activité de l'entreprise : des cyberattaques peuvent entrainer de lourdes pertes économiques et financières et nuire à l'image de l'entreprise.

D'autre part**, les vulnérabilités des systèmes d'information sont de plus en plus nombreuses. Les nouveaux usages des TIC liés à la mobilité (utilisation de smartphones, de tablettes) sont beaucoup moins robustes en matière de sécurité que les ordinateurs classiques**. Le développement du BYOD (*Bring your own device*), qui consiste à utiliser son appareil personnel au travail est LE nouveau cauchemar des DSI. C'est un phénomène extrêmement complexe à gérer, en raison de la diversité des appareils, et des problèmes que génère l'enchevêtrement des usages privé et professionnel. **Beaucoup de questions se posent aussi autour de la sécurité du *cloud computing*, qui se développe fortement et devrait représenter un marché de 150 Milliards de dollars en 2014** (selon le cabinet de conseil Gartner). **Enfin, le problème le plus difficile à gérer est sans doute lié aux vulnérabilités humaines** : les individus sont souvent peu conscients du niveau de la menace informatique et ils ignorent ou contournent les mesures basiques d'« hygiène informatique » destinées à réduire le risque.

La prise de conscience politique des enjeux de la cybersécurité a progressé au cours de la dernière décennie.

En France, le Livre Blanc sur la défense et la sécurité nationale de 2008 a impulsé une dynamique à la cybersécurité et a abouti à **la création en 2009 de l'Agence nationale de la sécurité des systèmes d'information (l'ANSSI)**, en remplacement d'une ancienne structure (la DCSSI), avec une extension des compétences et des moyens mis à sa disposition. Les États-Unis sont été le premier pays à accorder une priorité stratégique à la protection des systèmes d'information : dès 1998, le Président Clinton signait un décret sur la protection des infrastructures critiques. Le Royaume-Uni a également fourni un effort important en 2011, avec notamment un travail de sensibilisation auprès des dirigeants des plus grandes entreprises du pays.

Au niveau européen, une agence, **l'ENISA, intervient principalement en soutien des pays les plus en retard dans le domaine**. **Le plan stratégique européen et la proposition de directive témoignent cependant de la volonté récente de la Commission européenne de s'emparer de ce sujet.**

Sur le plan international, **les tentatives de coordination se heurtent à des désaccords de fond entre les États** sur la régulation d'internet et des débats récurrents autour du degré d'ouverture et de contrôle d'Internet, et du caractère non démocratique de cette régulation.

Malgré cette prise de conscience, le niveau de protection contre les cyberattaques est toujours insuffisant comme l'a rappelé le rapport du sénateur Bockel de juillet 2012. **La présente Note d'analyse formule quatre recommandations destinées à élever le niveau de sécurité des systèmes d'information.**

Tout d'abord, et c'est un enjeu de souveraineté nationale, **la sécurité des opérateurs d'importance vitale (OIV) doit être accrue.** Ces opérateurs, identifiés par la législation, interviennent dans de nombreux secteurs de l'économie : les activités stratégiques de l'État, les réseaux de transport et d'énergie, la finance, etc. **Afin d'améliorer leur résilience face aux attaques et d'assurer la continuité de l'activité économique, la réglementation vis-à-vis de ces opérateurs doit être plus contraignante avec notamment :**

- l'obligation de s'équiper de systèmes de détection d'attaques labellisés ;
- la participation obligatoire aux tests de cybersécurité mis en œuvre dans le cadre national et européen.

L'ANSSI, qui a seulement un rôle de conseil auprès de ces OIV, doit être dotée d'un pouvoir de contrôle sur la mise en œuvre de cette réglementation.

Ensuite, il est important de reconnaitre la difficulté du travail des responsables de la sécurité des systèmes d'information (RSSI) : le personnel et les dirigeants ne sont pas sensibilisés au risque informatique et les usages mobiles peu sécurisés se développent massivement. Mais les RSSI ne peuvent aller à l'encontre de ces évolutions au risque de créer des pratiques de contournement encore plus dommageables en termes de sécurité. **Afin de concilier la sécurité et l'ouverture des systèmes d'information et d'accompagner les nouveaux usages, une démarche de gestion des risques doit être promue.** Elle consiste à hiérarchiser les menaces, les vulnérabilités et les informations à protéger, afin de mettre en œuvre une réponse adaptée à chaque entreprise, à la fois sur les plans technique et organisationnel. **Mais les TPE/PME ne disposent pas des ressources humaines ou financières pour se protéger correctement. L'ANSSI et / ou une association comme le CLUSIF (Club de la sécurité de l'information français) pourraient développer et mettre à la disposition de ces entreprises des outils simples pour gérer les risques.**

La **troisième recommandation** part du constat que la sécurité des systèmes d'information est principalement envisagée du point de vue national : **l'indépendance de l'offre de produits et services de sécurité est donc un enjeu fort**. Mais malgré des compétences académiques reconnues internationalement (en cryptologie notamment), **la France accuse un certain retard dans ce domaine de la science informatique et de la sécurité**. Le tissu industriel des produits de sécurité est trop éclaté et peine à atteindre une taille critique. **Le rôle de l'ANSSI**

pour accompagner l'offre française de solutions de sécurité doit être accru, afin de soutenir des initiatives privées et de faire émerger des partenariats. Le soutien au projet d'antivirus français DAVFI, par l'ANSSI sur le plan technique et dans le cadre des investissements d'avenir au niveau financier, est à cet égard exemplaire. La sécurité des systèmes d'information, il faut le rappeler, fait partie des 5 technologies qualifiées de stratégiques par la feuille de route du Gouvernement sur le numérique, et qui seront soutenues par le PIA.

Enfin, la recherche dans le domaine de la sécurité informatique est entravée par de nombreux blocages juridiques, et notamment :

- l'interdiction de la rétroingénierie pour motif de sécurité ;
- l'interdiction de révéler une faille de sécurité publiquement (principe de la sécurité par transparence).

Il convient donc, **sous le contrôle de l'ANSSI et d'un comité d'éthique *ad hoc*, de réfléchir aux moyens de conduire des expérimentations pour tester la sécurité de logiciels propriétaires et traiter des attaques informatiques.**

Élever le niveau de sécurité des systèmes d'information est une urgence, qui nécessite d'agir à de nombreux niveaux (éducation et formation, sensibilisation, soutien technique et méthodologique, réglementation) afin d'améliorer la résilience de notre économie face aux cyberattaques.

• **Contact Presse**
Centre d'analyse stratégique
Jean-Michel Roullé
Responsable de la communication
Tél. : +33 (0) 1 42 75 61 37
jean-michel.roulle@strategie.gouv.fr