Centre **risque & performance**

ÉCOLE POLYTECHNIQUE MONTRÉAL

Bulletin d'information mars – avril 2009 Vol. 7 No. 2

Le problème de la cybersécurité

La vulnérabilité cybernétique des infrastructures essentielles

La prise en compte de la cybersécurité est de plus en plus d'actualité. En effet, au cours des dernières années, l'outil cybernétique est devenu plus sophistiqué et plus ciblé ce qui entraîne de nouvelles menaces pour le fonctionnement des systèmes supportant la sécurité civile.

Aux États-Unis, le président Obama a récemment demandé au *National Security and Homeland Security* un examen de la manière dont est prise en compte la cybersécurité par les différentes agences américaines de manière à pouvoir mettre en œuvre une stratégie de sécurisation du cyberespace tout en conservant les droits et libertés des citoyens américains.

Cette demande du président américain fait suite aux conclusions du rapport de la *Commission on Cybersecurity for the 44th Presidency* du *Center for Strategic and International Studies (CSIS)*. Ce rapport réalisé en décembre 2008 précisait que la protection du cyberespace est le problème de sécurité le plus urgent auquel doit faire face la nouvelle administration Obama tant les menaces reliées aux cyberattaques peuvent affecter les infrastructures essentielles et par la même l'économie de la société civile. La prise en compte des risques cybernétiques s'est essentiellement effectuée par l'analyse des conséquences physiques qu'ils pourraient engendrer. Il apparaît actuellement plus important de considérer les effets au niveau informationnel. En 2007, de nombreuses institutions américaines (NASA, Homeland Security, etc.) ont subi des intrusions de leurs réseaux ciblant directement les échanges de données. Cela laisse craindre l'utilisation que pourraient faire de ces données les militaires et les différentes agences de renseignement. L'exploitation des vulnérabilités des infrastructures cybernétiques devrait être à la base de tous les conflits futurs.

Il convient donc de s'intéresser tout particulièrement à cette problématique. Il ne s'agit pas uniquement de s'assurer de la confidentialité des données ou de leur transfert. Il faut également considérer l'intégrité de ces données. Il faut donc aborder la protection du cyberespace d'un point de vue de sûreté de fonctionnement et non nous cantonner à l'aborder uniquement du point de vue de la sécurité informatique. Cette protection doit passer d'un mode adapté à l'ère industrielle à un autre adapté à l'ère de l'information. Cela nécessite donc une refonte en profondeur des institutions gouvernementales et privées. Ce constat, qui est valide pour les États-Unis, l'est également pour les autres pays. Il n'y a qu'à penser aux cyberattaques qu'a subies en 2007 le système de santé du Québec, mais également celles qui ont paralysé le gouvernement estonien. Cette problématique de cybersécurité est donc mondiale.

De manière à favoriser la refonte de la manière dont la cybersécurité est abordée par les États-Unis, le CCIS a émis de nombreuses recommandations. Parmi celles-ci, certaines abordent plus spécifiquement les infrastructures essentielles et en particulier les systèmes de contrôle à distance, tels que les systèmes SCADA. En effet, les infrastructures essentielles qui possédaient des systèmes de télécommunications indépendants ont de plus en plus tendance à utiliser des systèmes connectés à Internet. Il est important de sécuriser ces systèmes en développant des programmes de régulation et de recherche, mais également des programmes d'éducation. Ces recommandations qui sont valables pour les États-Unis pourraient également servir de base de réflexion pour le Canada.

Toutefois, il ne faut pas uniquement considérer la problématique des risques cybernétiques sous l'angle de la vulnérabilité face à des actes terroristes. Il est également important de considérer les vulnérabilités pouvant être reliées à un fonctionnement normal des systèmes et découlant d'autres types d'aléas. Il convient de mettre une emphase particulière sur la vulnérabilité des systèmes découlant de leur dépendance face à l'utilisation des données.

Frédéric Petit, doctorant, Centre risque & performance

Référence : Center for Startegic and International Studies (2008). Securing Cyberspace for the 44th Presidency – A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Center for Startegic and International Studies, Washington, DC, December 2008, 90 p. http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

À noter que Frédéric Petit défendra sa thèse de doctorat le 11 mars prochain au *Infrastructure Assurance Center* du *Argonne National Laboratory* de Chicago. La soutenance sera diffusée par vidéoconférence à 14h à l'École Polytechnique, salle B-529. Bienvenue à tous!
Info : 514-340-4711 p. 5927.

Nouvelles brèves du CRP

❶ La planification des événements majeurs au Canada

Le Programme technique de sécurité publique (PTSP) de Recherche et Développement Défense Canada vient d'approuver le financement d'un nouveau projet du CRP. Le projet vise à adapter et appliquer la méthodologie du CRP à l'évaluation des interdépendances entre les réseaux dans la planification des événements majeurs. Un cas concret sera utilisé pour valider la méthodologie : la planification du Sommet du G8 en Ontario en 2010. Le projet se fera en collaboration avec Sécurité publique Canada. Les travaux débuteront en avril 2009.

❷ Soutenance de maîtrise

Géraldine Guichardet, étudiante au CRP, soutiendra son mémoire de maîtrise en avril (date à confirmer). Son sujet de recherche est la caractérisation du raisonnement des experts pour l'anticipation et la modélisation des effets domino entre réseaux de support à la vie. Bienvenue à tous! Info : 514-340-4711 poste 5927.

Ce bulletin est publié par le *Centre risque & performance* de l'École Polytechnique de Montréal. Si vous désirez que votre nom soit ajouté ou retiré de la liste d'envoi, communiquez avec Irène Cloutier, tél. : 514-340-4711 poste 5927, courriel : irene.cloutier@polymtl.ca.

Les partenaires du *Centre risque & performance* : ***Agence Métropolitaine de Transport, Bell Canada, GazMétro, Hydro Québec, ministère de la Sécurité publique du Québec, ministère des Transports du Québec, Recherche & Développement Défense Canada, Sécurité publique Canada, Société de Transport de Montréal, Ville de Montréal (Centre de sécurité civile, Réseau d'aqueduc et d'égouts), Ville de Québec (Bureau de la sécurité civile).***