

# LE DEVOIR

Le Devoir

IDÉES, samedi, 19 février 2005, p. b5

## Il y a un problème avec toutes les infrastructures critiques!

Charles-Philippe David; **Benoît Gagnon**

Entre le rapport de la vérificatrice générale du Canada dénonçant les lacunes gouvernementales en matière informatique et le reportage de Radio-Canada sur les centrales hydroélectriques Manic-1, Manic-2, Manic-5 et LG-2, la question de la sécurité des infrastructures critiques a soudainement été portée sur le devant de la scène.

Il faut désormais dépasser la polémique pour s'interroger sur l'état de la sécurité en général de secteurs tels les services de santé, les banques, le nucléaire, les transports ou les télécommunications. Cette affaire révèle de fait une problématique beaucoup plus large et plus complexe que la seule sécurité des centrales hydroélectriques. Elle soulève en effet la question de toute la sécurité des infrastructures critiques, c'est-à-dire des centres névralgiques dont dépend notre mode de vie.

### Sentiment d'urgence

Pourtant, le 11 septembre 2001 avait constitué un électrochoc qui avait mené bon nombre d'experts en Amérique du Nord, notamment, à réfléchir à la protection de ces infrastructures. Le sentiment d'urgence qui prévalait alors s'est progressivement érodé sous l'effet des contraintes financières et de la gestion quotidienne: les constats ont été faits, les diagnostics établis, les solutions proposées, mais bien peu de mesures sont aujourd'hui en vigueur... au Canada comme aux États-Unis, d'ailleurs.

Aussi la plupart des centres névralgiques (tels l'électricité, les transports ou les banques) restent-ils des cibles relativement accessibles pour qui voudrait perturber la vie politique, économique et sociale d'un État. Il est possible - comme l'a récemment fait Richard Clarke dans *The Atlantic Monthly* - de multiplier à l'envi les scénarios d'attentats de grande envergure. Pour autant, et fort heureusement, peu se concrétisent car, règle générale, les terroristes obéissent à des motivations politiques et non criminelles.

Ce dernier constat ne doit toutefois pas conduire à l'indolence: il reste nécessaire, plus de trois ans après le 11 septembre 2001, de mettre sur pied des mesures préventives. C'est ce que l'Amérique du Nord dans son ensemble aurait dû conclure à la suite des attentats de Madrid, le 11 mars 2004. Et s'il y a eu quelques améliorations notables (notamment pour les installations aéroportuaires, mais les pressions américaines sont considérables ici), le Québec et le Canada ont accordé peu d'attention à cette question.

Et pourtant, le fait que de nombreuses infrastructures critiques du Québec appartiennent au secteur public constitue un atout pour déployer rapidement des mesures de sécurité efficaces et uniformes. Cette situation est bien différente des États-Unis, où la majorité des infrastructures sont aux mains de sociétés privées dans les affaires desquelles l'État répugne à s'ingérer.

### Les réalités de la sécurité informatique

Si la sécurité des infrastructures critiques peut être aisément assurée de manière classique, il n'en est pas de même de sa dimension informatique: les scénarios de cyberattaques sont trop souvent absents des considérations des décideurs gouvernementaux et privés. C'est d'ailleurs ce manque d'intérêt et de ressources que relève la vérificatrice générale en soulignant les conséquences sur la perméabilité et la vulnérabilité du réseau informatique fédéral.

Des attaques informatiques bien planifiées pourraient porter atteinte à la sécurité des États. C'est ce que le ver informatique Code Red est venu confirmer en ébranlant, en juillet 2001, la sécurité des infrastructures économiques et bancaires mondiales. De telles intrusions ont même provoqué la faillite directe d'entreprises, comme en atteste la fermeture, en février 2002, de la compagnie CloudNine Communication, ses dirigeants ayant estimé que la réparation des réseaux nécessitait trop d'investissements.

La dépendance de nos sociétés aux technologies de l'information crée de nouveaux types d'intrusions car il est désormais possible de déstabiliser à moindre coût une société en paralysant ses infrastructures critiques.

Des efforts à faire

Il faut assurément continuer à «repenser la sécurité» et, à ce titre, le reportage du journaliste Christian Latreille a le mérite de relancer le débat. Il faut dès lors dépasser la question des seules infrastructures hydroélectriques pour comprendre que, désormais, bien des barrières physiques et informatiques peuvent être franchies.

Les décideurs doivent prendre conscience que toutes les infrastructures sont vulnérables et que des efforts de prévention, peu spectaculaires mais efficaces, doivent être mis en oeuvre. Il ne s'agit toutefois pas de céder à la panique car, de toute évidence, les infrastructures canadiennes ne sont pas une cible prioritaire du terrorisme international.

En même temps, on ne peut pas se leurrer: l'interdépendance de nos infrastructures critiques, les connexions entre les réseaux, le lien étroit entre la sécurité informatique et la sécurité physique dans les centres névralgiques créent également un grand nombre de failles, autant de brèches potentielles qui ne pourront toutes être colmatées. Car l'invulnérabilité appartient à la science-fiction. Tout comme les scénarios terroristes... jusqu'à ce qu'ils se réalisent.

*Charles-Philippe David : Titulaire, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal*


*Benoît Gagnon : Chercheur spécialisé sur la protection des infrastructures, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal*

*Benoît Gagnon : Les auteurs ont contribué à l'ouvrage Repenser la sécurité (Fides, 2002).*

© 2005 Le Devoir. Tous droits réservés.

Numéro de document : news·20050219·LE·75225

---

 news·20050219·LE·75225

Ce certificat est émis à **Université-de-Montréal** à des fins de visualisation personnelle et temporaire.

Date d'émission : **2007-11-22**

Le présent document est protégé par les lois et conventions internationales sur le droit d'auteur et son utilisation est régie par ces lois et conventions.