TRÈS SECRET
Dossier nº : 2800-159
(TD R510)

L'ENQUÊTE DU SCRS CYBERMENACE

(ÉTUDE N^{O} 2010-07 DU CSARS)

Comité de surveillance des activités de renseignement de sécurité
23 juin 2011

La traduction de tous les examens du CSARS a été officiellement complétée par le Bureau de la traduction du Canada. En cas de litige, la version faisant autorité de la spécification est le document original en anglais.

TABLE DES MATIÈRES

1 INTRODUCTION

Depuis longtemps, le Canada est la cible d'activités d'espionnage étranger en raison de ses capacités scientifiques et technologiques, Récemment, le directeur du SCRS a déclaré que le Canada connaît des niveaux d'espionnage comparables à ce qu'on pouvait observer au plus fort de la Guerre froide[1], y compris des opérations d'information ou des « cyberattaques ». Il n'est pas étonnant que les cybermenaces, sont maintenant une priorité pour le gouvernement du Canada. Par conséquent, le SCRS a été chargé de fournir

À l'automne 2010, le gouvernement a lancé la *Stratégie de cybersécurité du Canada*. Cette stratégie pangouvernementale définit les rôles et les responsabilités des ministères et organismes fédéraux à l'égard d'un large éventail d'enjeux touchant la cybersécurité, y compris le cyberespionnage. Étant donné son expertise et son mandat, le Centre de la sécurité des télécommunications Canada (CSTC)[3], organisme responsable du renseignement d'origine électromagnétique, joue un rôle clé. Dans le cadre de la stratégie, le CSTC est chargé de renforcer sa capacité de détecter et de découvrir des menaces et de réagir aux cybermenaces et attaques contre les réseaux de communication et les systèmes informatiques du gouvernement.

---

1 Voir le documentaire sur le SCRS de la CBC : entrevue avec Brian Stewart, 22 avril 2010.

3 On entend par « renseignement d'origine électromagnétique », ou SIGINT, l'information obtenue grâce à l'interception de communications, de transmissions radar ou de transmissions de données.

Afin de pouvoir réaliser son propre mandat, réitéré dans la *Stratégie*, le SCRS a élaboré une approche en deux volets

Dans le cadre de la présente étude, le Comité examine l'enquête du SCRS sur la cybermenace posée et, de façon générale, la façon dont les efforts déployés par le SCRS contribuent à la cybersécurité du Canada. Tout d'abord, nous examinons la menace ainsi que certains défis clés associés à son enquête. Ensuite, nous étudions de plus près les stratégies et les outils que le SCRS utilise pour faire avancer l'enquête, approche renouvelée du SCRS pour cybermenaces établit des jalons clairs qui permettront d'évaluer le succès de l'enquête. Enfin, nous explorons le rôle du SCRS dans le contexte d'une approche « pangouvernementale » globale visant à contrer les cybermenaces. Cette analyse donne à penser que le SCRS, lorsqu'il se positionnera pour l'avenir, devrait demeurer aligné sur le rôle d'enquête qui lui est attribué par le gouvernement et par la loi.

2 MÉTHODE ET PORTÉE

Aux fins de la présente étude, le CSARS a examiné et la politique du SCRS. Le CSARS s'est également penché sur des documents liés à la création et à la mise en œuvre de la *Stratégie de cybersécurité du Canada* ainsi qu'à la collaboration du Service avec d'autres ministères fédéraux, avec le secteur privé canadien et avec le milieu de la recherche. En outre, le CSARS a accès à plusieurs séances d'information tenues par

La période visée par la présente étude s'étend du 1er janvier 2007 au 31 août 2010, mais le Comité a pris en compte afin d'élargir sa compréhension des principaux enjeux.

3 MENACE LIÉE AU CYBERESPIONNAGE DE

3.1 La cyberattaque : une forme moderne de contre-espionnage

Au cours des dix dernières années, la menace posée par l'espionnage s'est étendue à l'espace virtuel en raison de l'accroissement de l'expertise et des capacités techniques . Cependant, le cyberespionnage n'est qu'une façon plus moderne d'arriver aux mêmes fins que l'espionnage « classique », c'est-à-dire la collecte d'information sur un État par un autre État. De plus,
le cyberespionnage s'attache également à contrer

Le cyberespionnage présente certains avantages par rapport à l'espionnage classique : le faible coût par comparaison à la formation et à la mobilisation d'espions humains; la capacité de s'attaquer aux maillons faibles d'un réseau de grande taille, et la difficulté d'identifier avec précision l'auteur d'une cyberattaque

3.2 Défis

5 RÔLE DU SCRS DANS LA STRATÉGIE DE CYBERSÉCURITÉ DU CANADA

À l'automne 2010, le gouvernement a lancé la *Stratégie de cybersécurité du Canada* afin de s'attaquer à la criminalité et aux menaces à la sécurité dans le monde virtuel. Le document énonce trois grands objectifs : premièrement, créer une approche centralisée complète relative aux cybermenaces; deuxièmement, décrire le rôle que doit jouer chaque ministère ou organisme dans l'effort pour contrer ces menaces; troisièmement, soutenir et renforcer les structures existantes qui se consacrent déjà à la cybersécurité[22].

La stratégie souligne l'importance des partenariats intérieurs à l'égard des enjeux touchant la cybersécurité[23]. Du point de vue du SCRS, la relation avec le CSTC est particulièrement cruciale, puisqu'il s'agit de l'organisme responsable de protéger les réseaux et les systèmes informatiques du gouvernement et de fournir des conseils relativement à l'atténuation des risques.

---

22 La *Stratégie* insiste également sur le renforcement des structures existantes visant à lutter contre les cybermenaces, comme le Centre canadien de réponse aux incidents cybernétiques (CCRIC), [TRADUCTION] « point de coordination des interventions relatives à des cyberincidents ».

23 La GRC doit « [enquêter] sur les actes criminels d'origine canadienne et étrangère impliquant des réseaux et des infrastructures essentielles d'information au Canada ». Gouvernement du Canada, *Stratégie de cybersécurité du Canada : renforcer le Canada et accroître sa prospérité*, 2010.

5.1 Enjeu à prendre en considération

Conformément à son mandat, et comme le précise la *Stratégie*, le rôle du SCRS est d'« analyse[r] les menaces nationales et étrangères mettant en péril la sécurité du Canada et [de mener] des enquêtes à ce sujet ». Le SCRS compte donc parmi les nombreux intervenants qui appuient les efforts globaux déployés par le gouvernement

L'atténuation, c'est-à-dire la fourniture de conseils aux victimes ou aux victimes potentielles dans les organismes gouvernementaux désignés, ne s'inscrit pas dans le mandat du SCRS en la matière.

Toutefois, **le SCRS devrait, lorsqu'il se positionne afin de pouvoir suivre la menace , demeurer aligné sur son rôle d'enquêteur et continuer de se garder de mener des activités susceptibles d'être considérées comme étant de l'atténuation.**

6 CONCLUSION

À la lumière de son examen de la nature de la cybermenace ainsi que des stratégies et des outils conçus par le Service, la présente étude décrit certains des défis et des débouchés liés à l'enquête. En outre, l'étude aborde les limites continues du rôle que peut jouer le Service dans le cadre d'une stratégie « pangouvernementale » —