La cybersécurité dans le secteur financier comme enjeu de sécurité économique

Mémoire présenté au Comité de la sécurité publique et nationale de la Chambre des communes

Professeure Jill Slay, présidente de la cybersécurité La Trobe Optus

Introduction

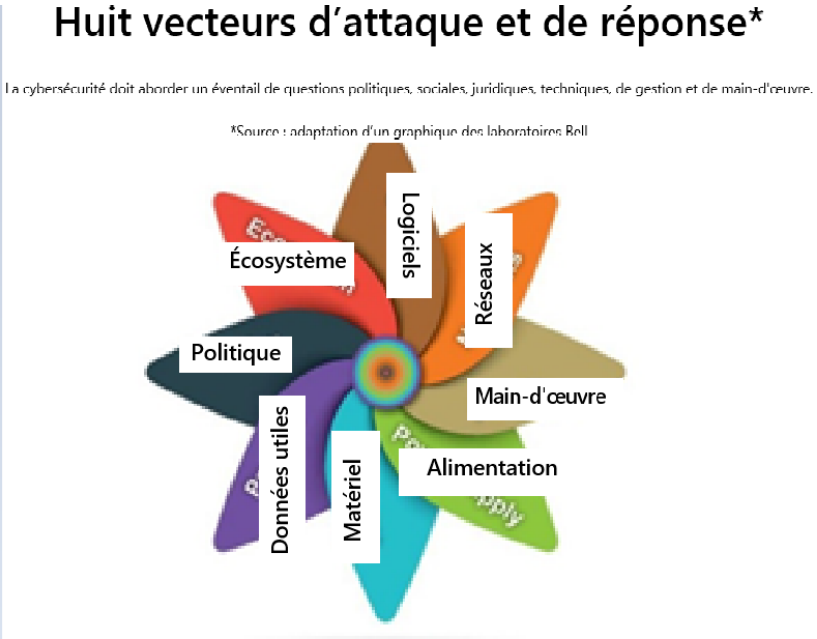
Dans ce mémoire, j'examine certains des principaux défis en matière de cybersécurité auxquels, je crois, l'Australie et le Canada (et, dans une certaine mesure, les autres partenaires du Groupe des cinq) sont confrontés et je présente des recommandations pour relever ces défis.

- Développement d'une compréhension claire de la nature des cybermenaces
- La cybersécurité dans le cadre de la sécurité nationale
- Élaborer un ensemble clair et culturellement adapté de certifications de cybersécurité nationale (résumé des travaux de l'Australian Computer Society)
- Élaborer un programme de recherche universitaire et gouvernemental approprié en cybersécurité, en particulier l'apprentissage automatique pour la cybersécurité, d'autres approches de l'intelligence artificielle et la sécurité de l'Internet des objets (IdO)

Contexte

L'un des principaux problèmes de cybersécurité auxquels l'Australie, le Canada et nos alliés font face est le grand nombre d'attaques contre le gouvernement, l'industrie et les utilisateurs à domicile. Bien que certaines soient ciblées et de grande valeur, la tendance générale est une croissance non confinée du niveau de menace et une croissance exponentielle des coûts économiques. Ces problèmes nationaux ont été mis en évidence en mai 2017 lors de la campagne du rançongiciel WannaCry. Selon un rapport d'Europol (2017), l'attaque a affecté environ 200 000 ordinateurs dans le monde en les chiffrant et en exigeant un paiement en cryptomonnaie. Au Royaume-Uni, le Service national de la santé à lui seul avait 70 000 appareils touchés, dont des appareils d'imagerie par résonance magnétique, des réfrigérateurs d'entreposage du sang et du matériel de salle d'opération. Selon une estimation, le coût économique mondial de WannaCry s'élève à quatre milliards de dollars.

La propagation de WannaCry a été interrompue en raison d'une limitation de la programmation, mais que se serait-il passé si cette limite n'avait pas existé? Et si WannaCry avait ciblé nos systèmes d'intérêt national? Mais surtout, comment l'Australie et le Canada vont-ils se défendre contre la prochaine version plus sophistiquée de WannaCry? Comment allons-nous aborder les questions du cyberrenseignement et de l'interprétation humaine de la menace que ce renseignement représente? Comment allons-nous réagir en cas d'attaque? Comment nos politiques de sécurité nationale appuient-elles la mise en œuvre d'une solution appropriée? Qui fera la recherche et la pratique dans ce domaine spécialisé?



Je pose ici un grand nombre de questions, mais en dix minutes, j'en aborderai trois.

Développement d'une compréhension claire de la nature de la cybersécurité

La cybersécurité est un terme qui est encore mal compris et qui est souvent assimilé à la « sécurité informatique et de réseau ». Or, nous devons tenir compte de la nature interdisciplinaire de la cybersécurité, y compris lorsque nous y réfléchissons sous l'angle de la sécurité économique.

La « cybersécurité » comporte au moins huit composantes fondamentales, dont certaines sont strictement techniques (mais concernent

des personnes et des organisations), tandis que d'autres sont simultanément techniques et profondément dépendantes d'intrants non techniques. Une illustration de ces ingrédients est saisie ici dans un graphique qui les décrit comme des vecteurs d'attaque et de réponse. Ce graphique est adapté d'une approche élaborée par les ingénieurs des laboratoires Bell pour régler les problèmes de défense des ordinateurs et des appareils connectés (Gupta et Buthmann, 2007). Ce concept permet de comprendre ce qui façonne la cybersécurité et la nature de la cyberdéfense. Mais il y a aussi une perspective nationale plus large, puisque la stratégie et la planification de la cybersécurité dépendent autant de l'environnement politique, juridique et social que des approches d'ingénierie et de systèmes, telles qu'elles sont conçues dans le travail original des laboratoires Bell.

La cybersécurité dans le cadre de la sécurité nationale

La cybersécurité est, pour certains du moins, encore une composante de l'informatique et une science théorique à la recherche de solutions formelles. Dans le milieu universitaire en particulier, le lien entre la cybersécurité, la cyberdéfense, l'espionnage et l'ingérence étrangère sont d'importants concepts liés qui commencent à peine à être compris.

La cybersécurité (ou la guerre cybernétique) pour la sécurité et la défense nationales est un concept relativement nouveau pour les experts techniques. La cybersécurité, en tant que problème de sécurité nationale, a été identifiée pour la première fois en Australie dans le Livre blanc sur la défense de 2000 (Défense 2000). En 2001, le gouvernement Howard a lancé une initiative de sécurité électronique, qui a permis de créer une collaboration entre les organismes du gouvernement fédéral et le Trusted Information Sharing Network (réseau de partage d'informations fiable), lequel représentait les principaux groupes sectoriels désignés comme infrastructures essentielles aux fins de la sécurité nationale (Parlement, 2013). Le gouvernement Rudd a examiné les politiques, programmes et capacités de l'Australie en matière de sécurité électronique en 2008. Le tableau ci-dessous résume les initiatives de cybersécurité depuis 2008, la source des politiques ou des conseils, ainsi que les répercussions sur la recherche et la main-d'œuvre professionnelle.

Besoin de cybersécurité	**Sources présumées de la politique ou des conseils**	**Conséquences pour la recherche sociotechnique**
• Cybersécurité • Guerre cybernétique et cyberdéfense • Cyberrenseignement et cyberespionnage	• Les 4 meilleures stratégies de l'Australian Signals Directorate (ASD, 2013) • Livre blanc sur la défense 2016 (Défense 2016) • Livre blanc sur la défense 2009 (Défense 2009) • Rapport de l'ASIO au Parlement 2011/2012 (ASIO, 2012) • Plan stratégique de l'ASIO 2013-2016 (ASIO, 2013)	Cohorte de chercheurs universitaires novateurs et de chefs de file du gouvernement/de l'industrie dans les domaines suivants : • Sécurité des réseaux et des données • Intervention en cas d'incident et informatique judiciaire • Développement de logiciels et ingénierie inverse • Effets cybernétiques • Renseignement de sources ouvertes • Lois et politiques • Relations internationales en matière de défense et de sécurité

- La politique et les conseils des 18 dernières années en Australie (et je crois que le Canada ne sera pas différent) montrent qu'il faut une main-d'œuvre hautement qualifiée pour relever les défis de la guerre cybernétique, de la cyberdéfense et de la cybersécurité et pour protéger tous les aspects de la société.
- Mes recherches, et mes connaissances du contexte australien, indiquent qu'il y a peu de recherches sur la cybersécurité pour la sécurité nationale australienne.
- Il n'y a pas de lien du secteur public entre le programme de sécurité nationale et les résultats de la recherche technique qui continuent d'être financés, mais qui ne sont pas nécessairement appliqués.
- Il n'existe pas de cadre établi sur lequel ce type de relation peut être fondée et, bien qu'il y ait de l'intérêt pour la réalisation de recherches sur de nouvelles questions difficiles comme les cyberopérations défensives, la cueillette automatisée de renseignements et de preuves cybernétiques, le leurre et certaines des questions humaines connexes, aucune recherche nationale crédible et soutenue n'est axée sur la mise en relation de la cybersécurité technique avec les visées nationales en matière de défense, de droit et de politiques.

Conseils

- Il faut créer (et mettre à l'essai et valider) un cadre pour préciser comment la cybersécurité et la cyberdéfense de l'économie canadienne et de son infrastructure essentielle pourraient être réalisées, en intégrant les perspectives techniques, sociotechniques et stratégiques.
- En l'absence de ce cadre, il faudra adopter une approche fragmentaire de la recherche universitaire sur la cybersécurité, c'est-à-dire s'appuyer sur les forces d'un chercheur ou d'un chef de recherche et sur la qualité de ses travaux antérieurs. Les études ainsi produites pourront être publiées dans un journal prestigieux, mais elles ne sauront fournir à la fois un contenu théorique à la fine pointe et des dispositifs ou techniques immédiatement utilisables et potentiellement commercialisables.

Normes professionnelles nationales en matière de cybersécurité, ensemble de connaissances commun, programmes d'études

L'Australian Computer Society est un organisme national d'accréditation informatique qui compte environ 40 000 membres. Il a élaboré un ensemble de normes professionnelles nationales en matière de cybersécurité afin que l'Australie puisse répondre aux questions « Qui est un professionnel de la cybersécurité? » et « Quel genre de compétences ces professionnels de la cybersécurité doivent-ils posséder pour répondre aux besoins de l'Australie? »

Normes professionnelles nationales

Elles ont été lancées en septembre 2017 dans le sillage des travaux effectués par le Groupe de travail sur la cybersécurité australienne (ACS) à la demande du conseiller spécial du premier ministre et chef du Australian Cyber Security Centre (ACSC), Alastair MacGibbon. Les normes ont été mises en œuvre, des évaluateurs ont été recrutés et formés et un nombre constant de nouveaux membres se prévalent maintenant de la possibilité de décrocher cette certification. Les candidats viennent de l'Australie et de l'Asie du Sud-Est et appartiennent aux divers domaines de la cybersécurité et de la TI. En résumé, les normes, tirées de la synthèse des travaux du NIST, de (ISC)^2 et d'ISACA, offrent une certification spécifique à l'Australie :

Professionnel certifié – Cybersécurité

Les exigences en matière d'évaluation de la spécialisation en cybersécurité sont équivalentes aux critères et cheminements d'évaluation des professionnels certifiés en matière de cybersécurité australienne; y est toutefois ajoutée la nécessité de démontrer une compétence approfondie dans quatre compétences du SFIA au niveau 5.

Les compétences applicables du SFIA sont les suivantes :

- Gouvernance de la TI
- Gestion de l'information
- Sécurité de l'information
- Assurance de l'information
- Gestion des risques de l'entreprise
- Test de pénétration

- Administration de la sécurité
- Programmation et développement de logiciels
- Logiciel d'exploitation
- Mise à l'essai
- Gestion des actifs

Technologue certifié – Cybersécurité

Les exigences en matière d'évaluation de la spécialisation en cybersécurité sont équivalentes aux critères et cheminements d'évaluation des technologues certifiés en matière de cybersécurité australienne; y est toutefois ajoutée la nécessité de démontrer une compétence approfondie dans trois compétences du SFIA au niveau 3.

Les compétences applicables du SFIA sont les suivantes :

- Gestion de l'information
- Sécurité de l'information
- Assurance de l'information
- Gestion des risques de l'entreprise
- Gestion du développement de systèmes
- Gestion des actifs
- Gestion du changement
- Administration de la sécurité
- Gestion des incidents
- Examen de la conformité

Enfin, nous avons deux projets d'élaboration de micro-titres de compétences et de lignes directrices pour les programmes d'études en cybersécurité. Je dirais que le Canada a besoin de la même chose pour déterminer la nature de la main-d'œuvre nécessaire et s'assurer que les programmes d'études correspondent aux besoins de cette main-d'œuvre. Je considère qu'il s'agit là des questions les plus importantes à discuter, mais je peux aussi répondre à des questions sur d'autres enjeux de recherche comme les infrastructures essentielles, l'IdO et les systèmes de déception.