Lutter contre les cybermenaces pesant sur les institutions financières au Canada: étude qualitative d'une approche de partenariat public-privé pour protéger des infrastructures critiques

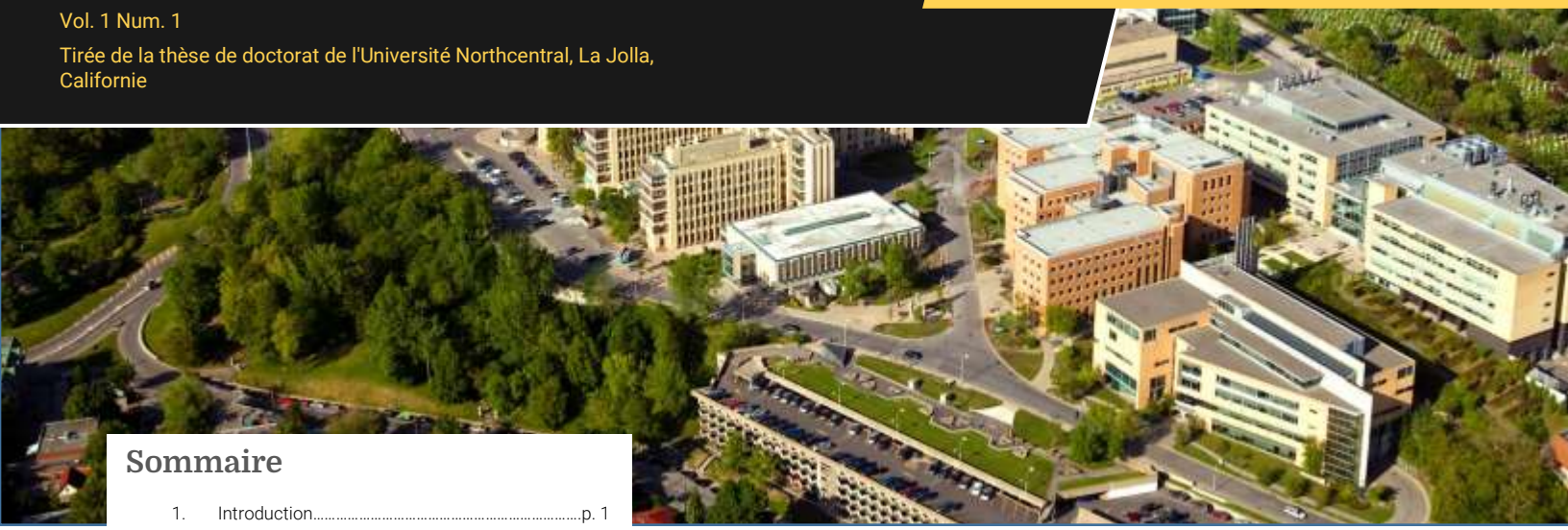
Pierre-Luc Pomerleau, Ph.D, MBA

Note de synthèse

Vol. 1 Num. 1

Tirée de la thèse de doctorat de l'Université Northcentral, La Jolla, Californie

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

1. Introduction....p. 1
2. Énoncé du problème....p. 2
3. Énoncé de l'objectif....p. 2
4. Résultat des entrevues....p. 3
5. Recommandations et leçons apprises....p. 4
6. Conclusion....p. 4
7. Références....p. 4

Pomerleau, P.-L. (2019). *Countering the Cyber Threats against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection* (Order No. 27540959). Repéré à https://www.proquest.com/products-services/pqdtglobal.html.

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

La protection des infrastructures est une responsabilité partagée entre le gouvernement et les entreprises privées qui collaborent pour en améliorer la résilience. En effet, la cybersécurité est un *bien public* qui doit être défini comme un problème nécessitant une action collective impliquant ces deux groupes d'acteurs[1]. Le secteur privé possède au Canada environ 80% des infrastructures critiques du pays et son rôle est essentiel dans la gestion des menaces qui touchent celles-ci[2] [3]. La sécurité intérieure relève de la responsabilité de divers groupes formés de « nœuds de sécurité » et d'acteurs issus des secteurs publics et privés[4].

Les conséquences des cyberattaques sur les infrastructures critiques peuvent avoir des impacts économiques, sociaux et environnementaux importants[5]. À l'heure actuelle, les professionnels canadiens de la sécurité bancaire ont mis en place une structure partenariale dynamique pour combattre collectivement diverses menaces auxquelles sont confrontées leurs organisations respectives, ce qui implique notamment un partage fluide d'informations. À ce titre, le secteur privé canadien s'adapte en temps quasi-réel aux changements rapides qui caractérisent les cybermenaces.

Même si les professionnels de la sécurité bancaire partagent des informations avec leurs homologues du secteur public, les renseignements ou alertes spécifiques qu'ils leurs transmettent demeurent conjoncturels,

omettant la majeure partie des données et des renseignements disponibles dans le secteur privé. Cette situation génère une myopie institutionnelle où le gouvernement ne dispose que d'une vision floue de l'état actuel des cybermenaces, ce qui augmente considérablement les risques pour les infrastructures critiques. Selon Carr[6], il subsiste un clivage fondamental entre les attentes des partenaires privés et publics concernant les rôles, les responsabilités et l'autorité dans la protection des infrastructures critiques face aux cybermenaces.

Énoncé du problème

Ces dernières années, les menaces à l'encontre des institutions financières ont changé. Ces menaces ne comprennent plus seulement des acteurs motivés par le profit, mais incluent également des acteurs étatiques et des groupuscules utilisant le cyberespace pour lancer des attaques contre les institutions financières[7]. Les statistiques de Sécurité Publique Canada montrent que les Canadiens sont victimes d'une attaque par rançongiciel environ 3200 fois par jour[8] [9]. Selon Statistique Canada[10], un cinquième des entreprises canadiennes ont été touchées par un incident de cybersécurité en 2017, et seulement 10% l'ont signalé aux forces de l'ordre. Le coût de la cybercriminalité au Canada équivaut à 0,17% de son produit intérieur brut (PIB), ce qui représente des pertes annuelles de 3,2 milliards de dollars canadiens par année[11]. De plus, les acteurs non étatiques continuent d'investir dans leurs cyber-capacités pour renforcer leurs attaques contre les institutions financières, ce qui constitue ainsi un risque majeur pour la sécurité nationale et la prospérité économique du Canada[12].

Il s'agit donc de comprendre pour quelles raisons les partenariats privé et publics (PPP) ont été inefficaces dans la surveillance, la détection et la réponse aux incidents de cybersécurité[13] [14].

La probabilité que les entreprises détectent des pirates informatiques est faible et le risque perçu d'arrestation semble minime pour les cybercriminels[15].

En raison de la nature internationale de la cybercriminalité, les forces de l'ordre éprouvent des difficultés à poursuivre les cybercriminels et à aider les banques à prévenir ces incidents[16]. Le secteur bancaire ne dispose pas des prérogatives de collecte du renseignement et des capacités nécessaires pour protéger ses réseaux et son infrastructure. À l'inverse, le gouvernement dispose de ces pouvoirs légaux et des capacités nécessaires, mais il ne dispose pas de l'expertise spécifique sur les cybermenaces affectant l'industrie financière[7] [15].

Énoncé de l'objectif

Dans cette étude qualitative, des entretiens avec des professionnels travaillant dans le domaine de la sécurité et de la cybersécurité pour les grandes institutions financières ont été menés afin de:

- Comprendre les facteurs contribuant à l'inefficacité du système actuel;
- Formuler des recommandations pour améliorer les partenariats publics et privés afin de protéger le secteur financier contre diverses cybermenaces;
- Déterminer si le cadre de gouvernance des réseaux de sécurité, proposé pour la première fois par Dupont[4] et adapté par Whelan et Dupont[17], permet de mieux comprendre le phénomène et d'identifier les meilleures pratiques de partage d'informations.

Les participants au sondage (N = 10) comprenaient des chefs de la sécurité et des chefs de la sécurité de l'information (ou leurs adjoints immédiats) travaillant pour des institutions financières canadiennes. Des entrevues (N = 9) ont été menées à Toronto et à Montréal. L'échantillon final représentait 23% des cadres supérieurs de sécurité des grandes institutions financières canadiennes. Cinq participants aux entrevues travaillaient pour l'une des six plus grandes banques du Canada.

Résultats des entrevues

Au total, 12 thèmes principaux sont ressortis de la collecte de données et de l'analyse des entretiens:

Thème 1: Pour prévenir les incidents, les professionnels de la sécurité des institutions financières doivent recevoir des informations ou des renseignements exploitables, et ils souhaitent les recevoir en temps quasi réel ou aussi fréquemment que possible.

Thème 2: Les participants ont expliqué qu'il est nécessaire de créer un centre de partage virtuel car les employés des secteurs publics et privés n'ont pas nécessairement besoin d'être présents physiquement au même endroit pour partager des informations entre eux.

Thème 3: Même si des rencontres en personne ont lieu entre les intervenants, les communications verbales par téléphone et l'échange de courriels sécurisés sont encore couramment utilisées entre les partenaires publics et privés. Selon les participants, les plateformes privées virtuelles seraient le mécanisme de communication le plus approprié pour échanger des informations en toute sécurité.

Thème 4: De manière unanime, les neuf participants aux entretiens ont souligné que le cadre juridique actuel était un défi majeur au partage d'informations avec le secteur public pour prévenir la criminalité contre les institutions financières.

Thème 5: En matière de prévention du crime, la plupart des participants ont mis en avant que les secteurs publics et privés ont des missions et des objectifs différents, ce qui réduit considérablement l'efficacité des PPP actuels.

Thème 6: Les participants à l'étude ont confiance en leurs collègues du secteur privé pour échanger des informations afin de les aider à prévenir la criminalité contre leurs organisations respectives. Cependant, les participants ont cité la confiance comme étant un frein au partage de l'information avec les parties prenantes du secteur public.

Thème 7: Étant donné que les entités privées telles que les institutions financières assument la plupart des risques du secteur financier, les rôles spécifiques que les secteurs privés et publics jouent en matière de protection des actifs des institutions financières ne sont pas clairs. Chaque institution financière assure sa propre sécurité, mais le gouvernement doit protéger l'industrie dans son ensemble.

Thème 8: La plupart des participants ont convenu que de multiples cyberattaques contre les banques dans un court laps de temps pourraient avoir des effets négatifs importants sur les investisseurs, les marchés boursiers, la confiance des clients dans le système financier ainsi que la réputation des organisations attaquées.

Thème 9: Les participants à l'étude ont estimé que le secteur financier devrait partager des informations avec d'autres infrastructures essentielles canadiennes, car certaines d'entre elles sont fortement interconnectées et dépendent donc les unes des autres. La plupart des participants ont souligné que le secteur bancaire est étroitement lié au secteur des télécommunications.

Thème 10: Au total, huit participants ont convenu qu'il était essentiel de continuer à accroître les capacités de partage d'informations entre les partenaires publics et privés.

Thème 11: les participants à l'étude conviennent que la structure du *Bank Crime Prevention and Investigation Framework (BCPIF)*, le modèle de gouvernance sous la gouverne de l'Association des banquiers canadiens pour le partage des informations entre les institutions financières membres, demeure le meilleur outil à leur disposition pour partager du renseignement.

Thème 12: Tous les participants ont confirmé que les PPP d'échange d'informations entre les institutions financières et le secteur public

devraient être classés comme des réseaux de sécurité selon la définition de Dupont[4]. Différents types de réseaux de sécurité sont nécessaires pour gérer efficacement la sécurité.

Recommandations et leçons apprises

Au total, 19 recommandations ont été formulées tout au long de cette étude. Les recommandations concernent la modification de la législation pour permettre le partage d'informations, la création de centres de partage, la clarification des rôles et des responsabilités des acteurs publics et privés, le mécanisme de partage des informations et la gouvernance de la sécurité. Les recommandations pratiques les plus importantes concernent quant à elles la modification de la législation afin de clarifier les rôles et les responsabilités, de faciliter le partage des informations entre les acteurs privés et publics à des fins de prévention, le partage des informations en temps opportun, et de créer un espace de partage sûr où les acteurs de la sécurité des deux secteurs seraient en mesure d'échanger des informations pour prévenir la criminalité, protéger les infrastructures critiques telles que les institutions financières et renforcer la sécurité nationale.

Un total de onze recommandations pour de futures études ont été identifiées tout au long de cette étude. Les recherches futures devraient se pencher sur les approches que les réseaux de sécurité peuvent adopter pour accroître l'efficacité et l'efficience de la gouvernance de la cybersécurité et de la criminalité financière[19]. Les cadres juridiques en vigueur au Royaume-Uni et aux États-Unis, ainsi que les facteurs de succès de projets de PPP tels que la National Cyber-Forensic and Training Alliance (NCFTA), le Financial Services Information Sharing and Analysis Center (FS-ISAC), le National Cybersecurity and Communications Integration Centre (NCCIC), et le Joint Money Laundering Intelligence Taskforce (JMLIT) devraient être davantage évalués. Les approches fondées sur le recours aux données probantes dans le contexte des institutions financières et des mesures de cybersécurité devraient également être priorisées afin d'évaluer les outils et les politiques les plus fréquemment utilisés par les réseaux de sécurité pour atteindre leurs objectifs, gérer les incidents de cybersécurité et enquêter sur les cybercrimes contre les institutions financières. Il n'existe en effet pas d'outils universellement acceptées pour mesurer l'efficacité des contrôles et des politiques de sécurité[19 20 21 22].

Conclusion

Cette étude a abordé le problème central de l'inefficacité des partenariats public-privé. La législation est un défi majeur pour les PPP canadiens. Le cadre de gouvernance des réseaux de sécurité proposé pour la première fois par Dupont[4] et adapté par Whelan et Dupont[17] permet de mieux comprendre ce phénomène, ainsi que d'identifier les meilleures pratiques pour les futurs PPP de partage du renseignement. Un total de 12 thèmes importants, 19 recommandations pratiques et 11 recommandations pour de futures recherches ont été identifiés dans cette étude.

Références

[1] McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5-12.
[2] Etzioni, A. (2017). The fusion of the private and public sectors. *Contemporary Politics*, *23*(1), 53–62.
[3] Vroegop, R. (2017). *The state of information and intelligence sharing in Canada*. The Conference Board of Canada.
[4] Dupont, B. (2004). Security in the age of networks. *Policing & Society*,*14*(1), 76.
[5] Mezher, T., El Khatib, S., et Sooriyaarachchi, T. M. (2015). Cyber-attacks on critical infrastructure and potential sustainable development impacts. *International Journal of Cyber Warfare & Terrorism*, *5*(3), 1.
[6] Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.
[7] Borghard, D, E. (2018). *Protecting financial institutions against cyber threats: A national security issue.*
[8] Gendarmerie Royale du Canada. (2019). Rançongiciels.
[9] Tunney, C. (2019). *With ransomware on the rise, RCMP urging victims to 'be patient with police'.* CBC.
[10] Statistique Canada. (2018). L'incidence du cybercrime sur les entreprises canadiennes, 2017.
[11] Sécurité Publique Canada. (2018). La nouvelle stratégie de cybersécurité favorise la cybersécurité, l'innovation et la prospérité.
[12] Centre de la sécurité des télécommunications. (2018). *Centre canadien pour la cybersécurité: Évaluation des cybermenaces nationales, 2018*.
[13] Bures, O. (2013). Public-private partnerships in the fight against terrorism? *Crime, Law & Social Change*, *60*(4), 429-455.
[14] Dunn-Cavelty, M. et Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*, 179-187.
[15] Boes, S. et Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. *Cyber-physical security*, 185.
[16] Holt, J. T. (2018). Regulating cybercrime through law enforcement and

industry mechanisms. *Annals of the American Academy of Political and Social Science*, *679*(1), 140–157.

[17] Whelan, C. et Dupont, B. (2017). Taking stock of networks across the security field: a review, typology and research agenda. *Policing &* Society, *27*(6), 671-687.

[18] Rondelez, R. (2018). Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. *International Journal of Cyber Criminology*, 300–315.

[19] Maimon, D., Alper, M., Sobesto, B. et Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33.

[20] Wilson, T., Maimon, D., Sobesto, B. et Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829–855.

[21] Testa, A., Maimon, D., Sobesto, B. et Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology and Public Policy*, *16*(3), 687-726.

[22] Maimon, D., Testa A., Sobesto B., Cukier M. et Wuling, R. (2019) Predictably deterrable? The case of system trespassers. Dans G. Wang, J. Feng, M. Bhuiyan et R. Lu, (dir.), *Security, privacy, and anonymity in computation, communication, and storage*. Springer, Cham.