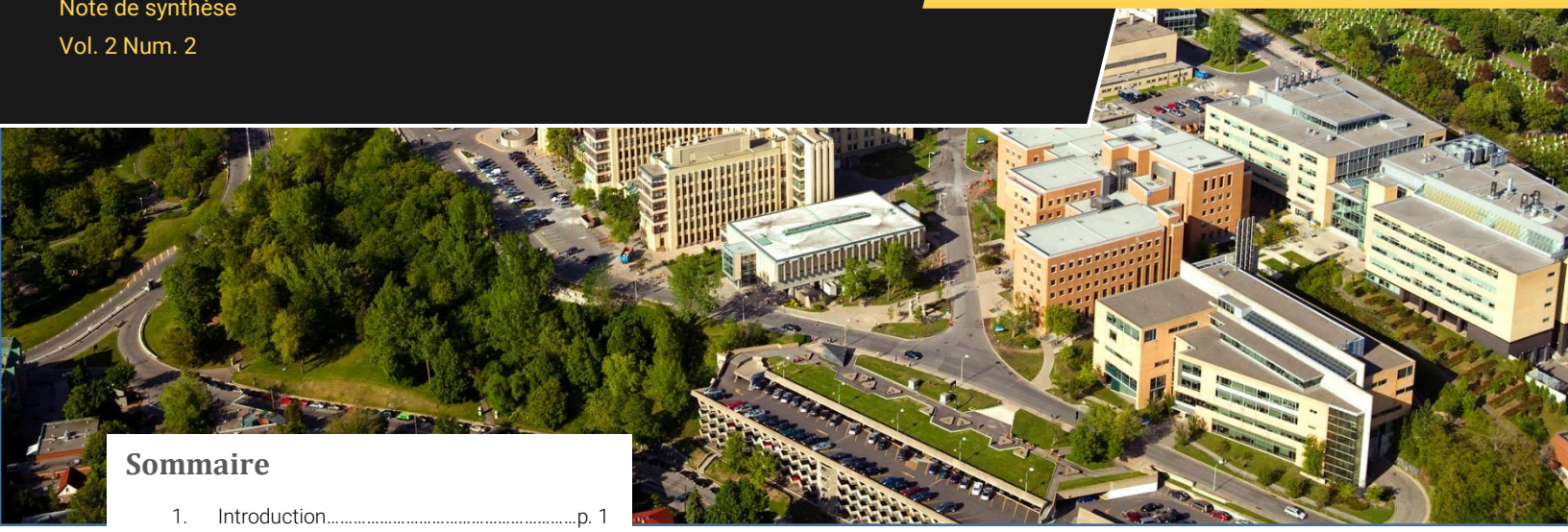
Les partenariats publics-privés en cybersécurité

Alexa Charles, candidate à la maîtrise

Note de synthèse
Vol. 2 Num. 2

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

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

Les institutions financières, et plus particulièrement les banques, font partie des infrastructures critiques d'un pays. Une infrastructure critique désigne **l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et services essentiels à la santé, à la sûreté, à la sécurité, au bien-être économique des Canadiens et au fonctionnement efficace du gouvernement**[1]. Les infrastructures s'appuient de plus en plus sur les nouvelles technologies, ce qui pose des défis importants pour les organisations qui doivent assurer la sécurité de leur système[2]. Dans ce contexte, un partage des informations et des renseignements efficaces et en temps utile entre le secteur public et les infrastructures critiques privées est plus qu'une nécessité[3]. La protection des infrastructures critiques fait aujourd'hui partie des stratégies de sécurité nationale à travers une approche de partenariat public-privé (PPP). Un PPP se définit comme **une relation organisée entre les organisations publiques et privées, qui établit des objectifs communs et des rôles distincts et qui met en place une méthodologie de travail pour atteindre des buts communs**[4].

L'importance des PPPs en cybersécurité est aujourd'hui largement reconnue par les décideurs politiques et l'industrie. En effet, bien que des entreprises privées soient responsables des infrastructures critiques, les gouvernements restent responsables de la définition et de la mise en œuvre des politiques publiques.

De cette façon, la coopération entre le public et le privé est essentielle pour maintenir un niveau élevé de sécurité des réseaux et de l'information[5]. De plus, les collaborations favorisent le partage d'information, améliorent les relations entre le secteur public et le secteur privé et mènent vers une meilleure compréhension des priorités, buts et contraintes de chacun. Cependant, des obstacles législatifs, corporatifs et culturels peuvent s'interposer dans la réalisation d'une collaboration efficace entre les infrastructures critiques privées et les agences gouvernementales[3]. Compte tenu de l'évolution rapide des cybermenaces, il est essentiel de pouvoir compter sur des canaux de partage de l'information efficaces et rapides entre le secteur public et le secteur privé.

Les fonctions et caractéristiques communes des PPPs

Il n'existe pas de modèle universel dans l'élaboration des PPPs, étant donné les différences culturelles, politiques et législatives entre les pays. Néanmoins, dans le contexte de la cybersécurité, il est possible de distinguer trois types de PPPs[5]:

- Les PPPs fondés sur la réponse (réactif) : Ces PPPs apportent une valeur immédiate et claire aux organisations privées et couvrent les phases de réponse et de récupération du cycle de la gestion des risques. Ces PPPs possèdent une orientation tactique et opérationnelle, et peuvent être mis en place pour répondre à un événement spécifique.

- Les PPPs fondés sur la prévention (proactif) : Ces PPPs couvrent les phases de prévention et de protection du cycle de la gestion des risques[6]. Ces PPPs prennent la forme d'une communauté à long terme coopérant selon une orientation stratégique et/ou tactique. Les organisations adhérant à ce type de PPPs doivent donc être capables d'adopter une vision à long terme. Les organismes publics peuvent amorcer ces PPPs, car non seulement leurs intérêts s'échelonnent sur le long terme, mais également ils contribuent de manière plus large aux intérêts nationaux.

- Les PPPs « Parapluie »: Ces types de PPPs sont en mesure de fournir des capacités tout au long du cycle de vie de la sécurité. Ils peuvent donc être très vastes afin d'inclure des membres ayant les rôles et responsabilités nécessaires pour répondre au cycle complet de la gestion des risques.

Il existe plusieurs stratégies pour mettre en oeuvre et faire évoluer un PPP, les plus communes étant l'approche *top down* et l'approche *bottom up*.

- Dans une approche *top down*, l'initiative vient du gouvernement et il se charge de fournir les règles et les directives.

- Une approche *bottom up* par opposé s'opère lorsque l'industrie reconnaît un besoin et travaille sur un mode collaboratif pour créer le partenariat[4].

Les partenariats commençant par une approche *bottom up* ont plus de chance de réussir[4]. En effet, les formes rigides de PPPs dans une approche *top down* tendent à décourager le travail d'équipe et l'efficacité[7]. Un PPP forme un réseau de nombreux acteurs, qui ont souvent des objectifs et des intérêts différents. Le gouvernement n'est pas le seul acteur et il peut donc difficilement imposer unilatéralement sa volonté. En outre, si les deux parties subissent des contraintes strictes imposées par une structure de commandement rigide et distante, le PPP ne pourra pas répondre à la nature fluide des cybermenaces.

Les avantages des PPPs aussi bien pour le secteur privé que le secteur public sont nombreux, notamment en termes de partage d'expertise, de connaissance et de bonnes pratiques pour améliorer la résilience dans le cyber-écosystème[5]. Qui plus est, le secteur public peut profiter des ressources du privé (technologie, innovation, etc.) et ainsi avoir une meilleure compréhension de la protection des infrastructures critiques et de l'industrie en général. De son côté, le secteur privé peut bénéficier de ressources financières

provenant des budgets publics, et il peut aussi s'impliquer dans l'élaboration et l'amélioration des législations nationales[5].

Les enjeux des PPPs

Par définition, les PPPs exigent que les parties prenantes aient des objectifs qui se complètent, une confiance mutuelle, des objectifs et des stratégies claires, une répartition des risques ainsi qu'un partage explicite des responsabilités et de l'autorité[8]. Cependant, les données extrêmement sensibles et confidentielles que possèdent des infrastructures telles que les banques peuvent constituer un frein à la collaboration puisqu'elles sont plus réticentes à partager de l'information[9].

En effet, les institutions financières souhaitent avant tout protéger les informations confidentielles de leurs clients. Un incident pourrait donc avoir des répercussions négatives sur la réputation de ces institutions d'où la nécessité d'établir des relations de confiance. Le maintien de la confiance constitue d'ailleurs un des plus gros défis dans l'élaboration d'un PPP, en raison des motivations différentes des deux secteurs[3]. C'est pourquoi il est essentiel que les rôles et objectifs au sein du PPP soient clairement définis[10].

Les différences d'objectifs, de méthodes, de cultures, d'attentes ou d'intérêts peuvent également être considérées comme des enjeux importants, mais seulement si les parties ne sont pas capables de faire face à ces différences[10]. En effet, les organismes d'application de la loi veulent utiliser les informations pour poursuivre les délinquants. Les institutions financières de leur côté veulent utiliser ces informations pour protéger les éléments essentiels de leur organisation[9]. L'écart entre les motivations du gouvernement et du secteur privé nécessite des lois et des réglementations supplémentaires pour améliorer les pratiques de cybersécurité, car une approche volontaire de collaboration ne fonctionnera pas[11].

Enfin, les barrières légales peuvent empêcher l'échange d'information. Depuis les attentats du 11 septembre 2001, le Canada a mis en place des législations afin de faciliter le partage de renseignement. Cependant, les informations ne sont pas partagées dans les deux sens, car le gouvernement reste réticent à divulguer des informations sensibles au secteur privé. Le travail de renseignement est rarement clair, il existe souvent des masses de données qui ne sont utiles que lorsqu'elles sont analysées et placées dans un contexte spécifique. De plus, le gouvernement doit aussi veiller à ne pas partager certaines informations reçues par d'autres agences gouvernementales, de peur de perdre la confiance de ces dernières[9].

De nombreuses contestations juridiques peuvent également entraver à l'efficacité d'un PPP. Les principales difficultés concernent les différents régimes de conservation des données et le partage de preuves recueillies dans le cadre d'une enquête[11]. Dans l'Union européenne par exemple, des directives imposent aux entreprises d'informer les autorités lorsqu'elles sont confrontées à un incident de cybersécurité. Aux États-Unis la divulgation des renseignements se fait sur une base volontaire dans le cadre d'un PPP[12], mais l'adoption en 2015 de la loi sur le partage des informations en matière de cybersécurité (*Cybersecurity Information Sharing Act* (CISA)) encourage le partage d'informations par le secteur privé en permettant d'apaiser les craintes concernant la responsabilité liée au partage. Cependant, cette loi a peu contribué à améliorer l'état du partage d'information, mais a, au contraire, plutôt ajouté des obstacles en imposant des méthodes de soumission contraignantes[13]. Le CISA manque de précision sur la manière dont les organismes publics et privés doivent fonctionner entre eux et négligent des facteurs clés associés au partage tels que la gestion de la confiance, les mesures incitatives, ainsi que la réciprocité[13].

En cela, il est important de mieux comprendre les réglementations et la législation en matière de protection de la vie privée afin de mieux délimiter ce qu'il est autorisé de partager et ce qui ne l'est

pas[14]. Il est nécessaire de trouver un équilibre entre le partage d'information pour renforcer à la fois, la sécurité nationale et la protection de la vie privée des Canadiens[15].

Quelques exemples de PPPs dans le secteur bancaire

Aux États-Unis, **les centres d'analyse et de partage de l'information** (*Information Sharing and Analysis Center*) sont des organisations sectorielles à but non lucratif fournissant une ressource centrale pour la collecte d'information sur les cybermenaces, afin d'encourager le partage d'information entre le secteur public et le secteur privé.

Une initiative telle que le **Financial Services Information Sharing and Analysis Center (FS-ISAC)** est un exemple de collaboration efficace dans le domaine. Le FS-ISAC échange des indicateurs de menaces, de vulnérabilités et d'incidents. Un groupe d'analystes valide les informations sur les menaces et les envoie aux membres. Comme mode de communication, le FS-ISAC a adopté l'utilisation d'une plateforme automatisée de renseignement sur les menaces, le Traffic Light Protocol (TLP). Cette plateforme garantit la diffusion d'informations confidentielles ou sensibles et la limite à des publics appropriés en fonction de la sensibilité et de la source de l'information[16].

Le **National Cyber Forensics & Training Alliance (NCFTA)** également aux États-Unis a pour but d'identifier, de prévenir et de neutraliser les cybercrimes à travers une collaboration internationale[17]. La collaboration s'opère entre l'industrie privée, le milieu académique ainsi que les forces de l'ordre. Le NCFTA encourage l'échange rapide de renseignements sur les principales cybermenaces qui pèsent sur les intérêts des entreprises et sur les nouvelles cybertendances. Les efforts du NCFTA ont donné lieu à des centaines d'enquêtes criminelles et à des accusations déposées contre plus de trois cents cybercriminels dans le monde entier. Le NCFTA a également produit plus de cinq cents rapports de renseignement sur les menaces cybernétiques au cours des trois dernières années seulement[17]. La réussite de ce partenariat tient à la capacité de fournir une collaboration non gouvernementale à but non lucratif pouvant être utilisée par les gouvernements lorsque cela est autorisé, et permettant d'assurer la protection de la chaîne de possession des données qui pourraient être utilisées dans le cadre de futures poursuites pénales en ligne. Des modèles intersectoriels similaires sont nécessaires pour un partage efficace des données[17].

Au Royaume-Uni, le **Cifas** est un service de prévention de la fraude qui regroupe des organisations des secteurs privés, publics, et bénévoles[18]. Il s'agit d'une organisation à but non lucratif dirigée par un conseil d'administration dont le rôle est de définir l'orientation et les objectifs stratégiques, de mesurer les performances par rapport aux objectifs stratégiques et d'examiner les risques et les contrôles. Le Cifas gère deux bases de données principales sur la prévention de la fraude les plus importantes du Royaume-Uni : le National Fraud Database et le Internal Fraud Database. Ce partenariat permet de créer un environnement non concurrentiel de prévention de la fraude axé sur la collaboration

En Australie, le **Fintel Alliance, lancé par le Australian Transaction Reports and Analysis Centre (AUSTRAC)** a pour but de combattre le blanchiment d'argent ainsi que le financement du terrorisme[19]. Il regroupe 22 organisations du secteur public et privé, et est reconnu comme étant le premier partenariat public-privé de ce type. Lancé en mars 2017, il soutient à la fois les membres du secteur privé à identifier et à signaler les transactions suspicieuses ; mais également les membres des forces de l'ordre à arrêter et poursuivre les criminels et travailler avec le milieu académique pour développer des connaissances. Les membres fournissent des informations à Fintel Alliance par l'intermédiaire d'AUSTRAC (le hub) qui les diffuse aux autres membres en utilisant une plateforme sécurisée et contrôlée. Les membres ne peuvent pas partager directement des informations avec d'autres organisations membres, sauf si cela est légalement autorisé[19]. Le PPP possède également un centre d'innovation qui agit comme une sorte de « bac à sable créatif ». Cela permet aux partenaires de co-concevoir de nouveaux produits, services et systèmes financiers

qui pourraient améliorer les capacités de détection et d'analyse des renseignements du centre opérationnel. L'un des avantages non négligeables réside dans la possibilité de réduire le fardeau réglementaire du secteur[19].

Au Canada, le Canadian Cyber Threat Exchange (CCTX), créé en 2015, aide les entreprises et les clients à se protéger contre les cybermenaces. À ce jour, le CCTX comprend près de 130 organisations telles que des sociétés de télécommunications, des institutions financières, des compagnies d'assurance et de transport[20]. Les membres peuvent soumettre des données en format structuré ou non, par le biais d'un portail web[20]. L'organisation s'appuie sur les protocoles STIX et TAXII pour caractériser les données et les transférer électroniquement entre les membres afin de réduire l'intervention humaine[20]. Un aspect essentiel du partage des données entre les membres du CCTX réside dans le fait que les données sont anonymisées, ce qui signifie qu'une organisation qui reçoit les informations ne pourra pas identifier l'organisation qui les fournit[20].

Recommandations

Il est impératif de prendre en compte les enjeux et les facteurs de réussite d'une collaboration efficace. En outre, aussi bien les secteurs privés et publics ont besoin d'incitatifs et de motivations à partager les informations afin de pallier aux obstacles culturels et réputationnels[9]. Également, une réciprocité est requise, les informations et les renseignements doivent être partagés dans les deux sens. Pour ce faire, il apparaît essentiel qu'un nouveau cadre de sécurité pour la protection des infrastructures critiques soit mis en place[3].

Effectivement, la protection des infrastructures critiques regroupe une multitude d'acteurs. Cette pluralité fait en sorte qu'il est difficile d'identifier les responsabilités de chaque acteur au sein d'un partenariat, puisque les systèmes de gouvernance actuels ne prennent pas en compte cette pluralité. Un nouveau cadre de sécurité devrait être élaboré de manière à répondre à la fois aux préoccupations et aux intérêts des secteurs privés et public[3]. Plus précisément, elles devraient garantir que les entreprises d'infrastructures critiques de toutes tailles puissent se protéger contre les cybermenaces. Pour ce faire, les mesures doivent être élaborées de manière réfléchie afin d'éviter des mesures réactives à l'avenir[11]. Ce cadre doit également être flexible et adopter une approche *bottom up* afin d'être en mesure de gérer la complexité des cybermenaces[20]. Une approche de partenariat public-privé menée par l'industrie garantira que les mesures soient efficaces et bénéficient des ressources du gouvernement.

Le secteur public joue un rôle clé quant à la régulation de la structure et la mise en place des règles à suivre dans l'élaboration d'un PPP. La promulgation de nouvelles lois et le développement des processus coordonnés permettraient de mieux appréhender et gérer les cybermenaces pour les parties prenantes. De plus, les normes techniques de communication telles que STIX et TAXII devraient être utilisées pour partager de manière automatisée et en temps réel les données relatives à la cybercriminalité ainsi que les indicateurs de menace à la cybersécurité. Finalement, compte tenu de l'évolution rapide des cybermenaces et de leur nature internationale, les PPPs devraient avoir pour principal objectif d'accroître la résilience dans le secteur financier.

Limites des études

Il existe encore à ce jour trop peu de littérature sur la manière dont un PPP efficace devrait être structuré et gouverné. En effet, les défis juridiques, la protection de la vie privée ainsi que les risques liés à la réputation sont les obstacles les plus importants pour une collaboration efficace dans un partenariat public-privé. Pour autant, il n'existe pas de consensus quant à la manière de procéder pour améliorer cette collaboration[21]. Les principales conclusions tirées de la littérature sont que le concept de partage d'information et le cadre légal restent relativement flous. Pour cette raison, il est impératif de continuer les recherches, et plus spécifiquement de clarifier les aspects entourant la structure des PPPs auxquels participent les institutions financières.

Références

[1] Public Safety Canada. (2009). National strategy for critical infrastructure. Ottawa, ON :Sécurité publique. Repéré à : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctreng.pdf

[2] Dodge, C. et Burruss, G. (2020). Policing cybercrime: responding to the growing problem and considering future solutions. Dans R. Leukfeldt et T. J. Holt (dir.), *The human factor of cybercrime (Routledge Studies in Crime and Society* (pp. 339-358). New York, NY: Routledge.

[3] 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). Available from ProQuest Dissertations & Theses Global. (2320957957). Retrieved from https://www.proquest.com/products-services/pqdtglobal.html ¶

[4] European Union Agency For Network Information Security (ENISA). (2011). Cooperative models for effective Public-Private Partnerships: Good practice guide. doi: 10.2824/21641

[5] European Union Agency For Network Information Security (ENISA). (2017). Public Private Partnership: Cooperative models. doi: 10.2824/076734

[6] Le modèle du cycle de la gestion des risques agit à titre de guide afin de s'assurer que toutes les étapes concernant la sécurité et la résilience sont bien évaluées et analysées. Les composantes du cycle de la gestion des risques sont : La dissuasion, la protection, la détection, la réponse et la récupération. Les PPPs se concentrent sur ce cycle de trois manières, représentant les trois types de PPPs.

[7] Osborne, S. (2000). *Public-Private Partnerships: Theory and Practice in International Perspective*. New York, NY: Routledge

[8] 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(4), 179-187. doi:10.1016/j.ijcip.2009.08.006

[9] Quigley, K., Bisset, B. et Mills, B. (2017). Too critical to fail : How Canada manages threats to critical infrastructures. McGill-Queens University Press

[10] Clark, R., Hakim, S., Boes, S. et Leukfled, E. R. (2016). Cyber-physical security (vol. 3). New York, NY: Springer Berlin Heidelberg.

[11] Laughlin, C. (2016). Cybersecurity in critical infrastructure sectors: a proactive approach to ensure inevitable laws and regulations are effective, 14(26).

[12] Wanca, I. (2014). Structuring public-private partnership for reducing cyber risk to critical infrastructure. Kindle Edition.

[13] Sedenberg, M, E., Dempsey, X, J. (2018). Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs. Repéré à : https://arxiv.org/abs/1805.12266

[14] Vroegop, R. (2017). The State of Information and Intelligence Sharing in Canada. The Conference Board of Canada.

[15] Shore, M, J, J., et Schafer, C. (2015). Review of commissions of inquiry with respect to findings of Major, O'connor, Iacobucci concerning information sharing that affects critical infrastructure protection. Critical information protection – Information sharing protocol project, CSSP-2013-CP-1026. Repéré à : http://cradpdf.drdcrddc.gc.ca/PDFS/unc199/p801

[16] Borden, M, R., Mooney, A, J., Taylor, M., & Sharkey, M. (2018). Threat information sharing and GDPR: A lawful activity that protects personal data.

[17] Plesco, R., Schneck, P. (2011). Criminal Public-Private Partnerships: Why Can't We Do That. Georgetown Journal of International Affairs, 151-154.

[18] CIFAS.(2020). *What is cifas*. Repéré à https://www.cifas.org.uk/about-cifas/what-is-cifas

[19] Chadderton, P., Norton, S. (2019). Public-Private Partnerships to disrupt Financial Crime: An Exploratory study of Australia's Fintel Alliance. Swift Institute.

[20] Shackelford, S. J. (2013). Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance. SSRN Electronic Journal. doi:10.2139/ssrn.2132526

[21] Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A., Rezek, C. (2015). Beyond Cybersecurity: Protecting your digital business. Wiley.