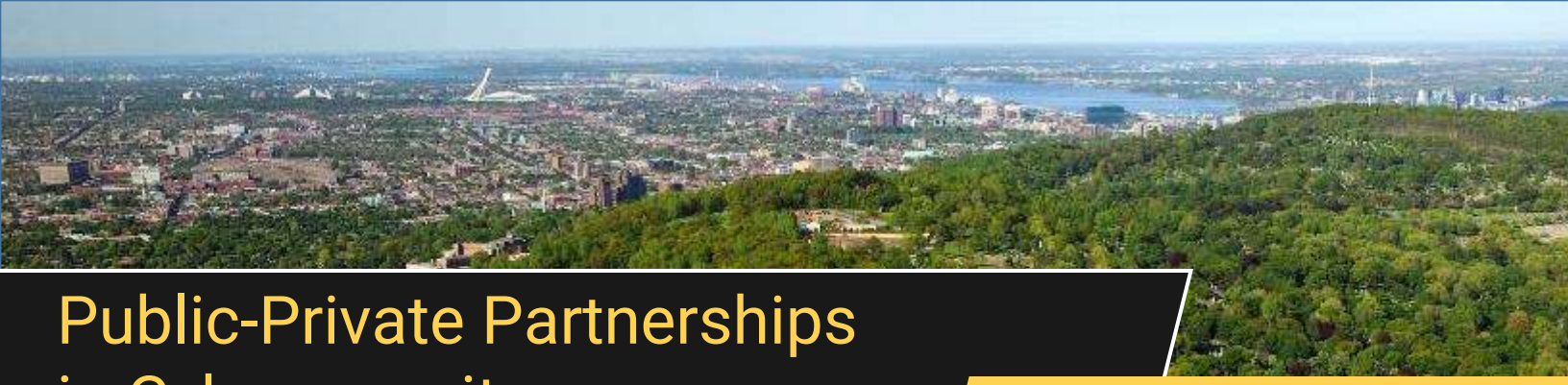
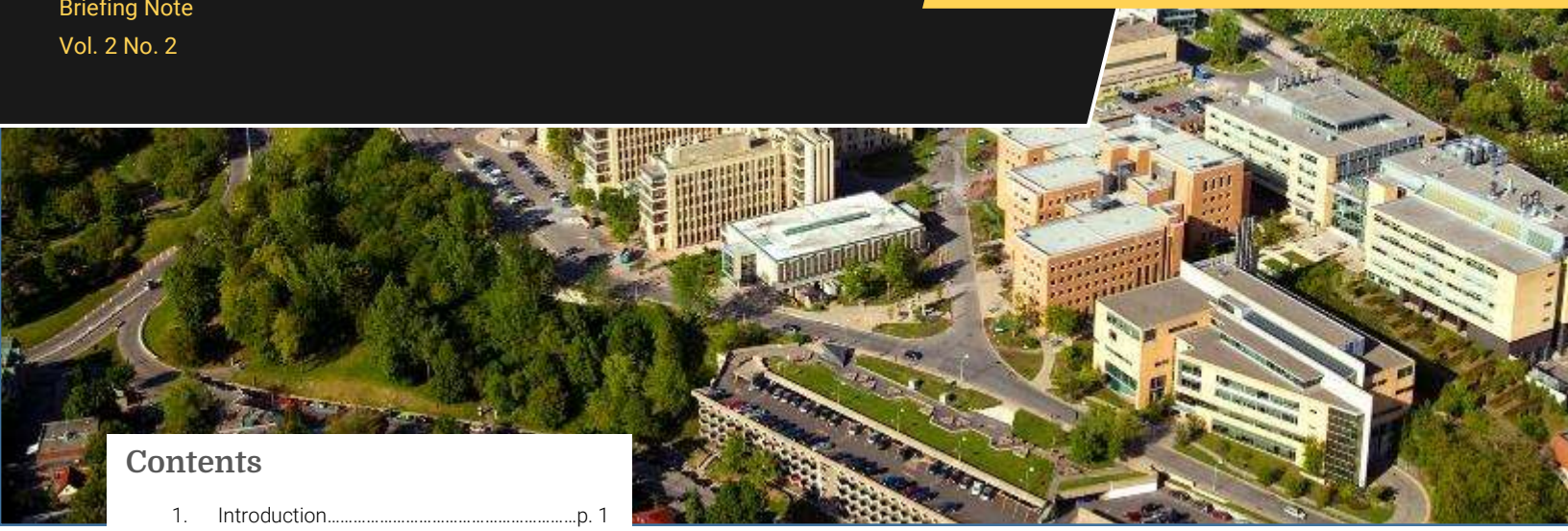


Public-Private Partnerships in Cybersecurity

Alexa Charles, Master's Candidate

Briefing Note
Vol. 2 No. 2

RCCP | Research Chair in Cybercrime Prevention



Contents

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Introduction

Financial institutions, particularly banks, are part of a country's critical infrastructure. Critical infrastructure refers to **all processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security and economic well-being of Canadians and the efficient functioning of government**.[1] Infrastructure increasingly relies on new technology, which poses significant challenges for organizations to ensure the safety of their systems.[2] In this context, effective and timely information and intelligence sharing between the public sector and private critical infrastructure is more than a necessity.[3] Protection of critical infrastructure is now part of national security strategies involving a public-private partnership (PPP) approach. A PPP is defined as **an organized relationship between public and private organizations in which the parties set common objectives, have separate roles and have an agreed-upon work method to achieve common goals**.[4]

The importance of PPPs in cybersecurity is now widely recognized by policy makers and industry. While private companies are responsible for critical infrastructure, governments remain responsible for defining and implementing public policies.

Thus, public-private cooperation is essential to maintaining a high level of network and information security.[5] In addition, collaboration fosters information sharing, enhances public/private sector relations and leads to a better understanding of each party's priorities, goals and constraints. However, legislative, corporate and cultural barriers can interfere with effective collaboration between private-sector critical infrastructure and government agencies.[3] With the rapid development of cyber threats, it is essential to have efficient and timely information-sharing channels between the public and private sectors.

Common functions and characteristics of PPPs

There is no one-size-fits-all model for PPPs, given the cultural, political and legislative differences between countries. Nevertheless, in the context of cybersecurity, three types of PPPs can be differentiated[5]:

- Response-based (reactive) PPPs: These PPPs provide immediate, clear-cut value for private organizations and cover the response and recovery phases of the risk management cycle. They have tactical and operational functions and can be set up to respond to a specific event.

- Prevention-based (proactive) PPPs: These PPPs cover the prevention and protection phases of the risk management cycle.[6] They are a long-term community where the participants cooperate based on a strategic and/or tactical function. Organizations involved in this type of PPP must be able to adopt a long-term vision. Public agencies can initiate PPPs because the PPPs serve their long-term interests and contribute to broader national interests.

- Umbrella PPPs: These types of PPPs can provide capabilities throughout the security life cycle. Therefore, they can be very broad in scope and include members with the duties and responsibilities required to implement the full risk management cycle.

There are several strategies for setting up and developing a PPP, the most common being the top-down and bottom-up approaches.

- With a top-down approach, the initiative comes from the government, which is responsible for providing the rules and guidelines.

- With a bottom-up approach, the industry recognizes a need and works on a collaborative method to set up the partnership.[4]

Partnerships starting with a bottom-up approach are more likely to be successful.[4] In fact, rigid forms of PPPs using a top-down approach tend to discourage teamwork and efficiency.[7] A PPP is a network of many players, often with different goals and interests. Because government is not the only player, it cannot easily impose its will unilaterally. Furthermore, if both parties are under strict constraints imposed by a rigid and distant command structure, the PPP will not respond to the fluid nature of cyber threats.

PPPs have many benefits for both the private and public sectors, particularly in sharing expertise, knowledge and best practices to make the cyber ecosystem more resilient.[5] The public sector can also benefit from private-sector resources (technology, innovation, etc.) and thus better understand critical infrastructure protection and the industry in general. For its part, the private sector can benefit from financial resources from public-sector budgets and be involved in drafting and improving national legislation.[5].

Challenges of PPPs

By definition, PPPs require stakeholders to have complementary objectives, mutual trust, clear objectives and strategies, risk allocation, and

explicit sharing of responsibilities and authority.[8] However, highly sensitive and confidential data held by infrastructure such as banks can be a barrier to collaboration as they are more reluctant to share information.[9]

Financial institutions want to protect their clients' confidential information above all else. An incident could therefore harm the reputation of these institutions, hence the need to establish relationships of trust. Maintaining trust is 1 of the biggest challenges in developing a PPP, because the two sectors have different motivations.[3] For this reason, it's essential that the roles and objectives within the PPP be clearly defined.[10].

Differences in objectives, methods, cultures, expectations or interests may also be considered important issues, but only if the parties are unable to deal with these differences.[10] Law enforcement agencies want to use the information to prosecute offenders. On the other hand, financial institutions want to use this information to protect the key components of their organization.[9] The disconnect between government and private-sector motivations requires additional statutes and regulations to improve cybersecurity practices because a voluntary collaborative approach won't work.[11]

Lastly, legal obstacles can prevent information sharing. Since 9/11, Canada has adopted legislation to facilitate intelligence sharing. However, information is not shared in both directions because the government remains reluctant to disclose sensitive information to the private sector. The purpose of intelligence work is often unclear, and masses of data are often useful only when analyzed and put into a specific context. In addition, the government must be careful not to share certain types of information received by other government agencies for fear of losing their trust[9].

Numerous legal challenges can also impede the effectiveness of a PPP. The main challenges concern different data retention regimes and the sharing of survey evidence.[11] In the European Union, there are guidelines requiring companies to inform authorities of any cybersecurity incident. In the US, disclosure of informations is voluntary under a PPP,[12]. Still, the *Cybersecurity Information Sharing Act* (CISA), adopted in 2015, sought to encourage information sharing by the private sector by alleviating concerns about liability for sharing otherwise legally restricted information. However, the law did little to improve the state of information sharing; if anything, it only added more hurdles by mandating cumbersome submission methods.[13] The CISA lacked specificity on how public and private bodies would work with each other and failed to address other key factors associated with sharing, including trust management, incentives and reciprocation.[13]

In that regard, it's important to better understand privacy regulations and legislation in order to better differentiate between what can and cannot be shared.[14] There is a need to balance sharing information to enhance national security with protecting the privacy of Canadians.[15]

Examples of PPPs in the banking sector

In the United States, **Information Sharing and Analysis Centers** are not-for-profit organizations that provide a central resource for gathering information on cyber threats to encourage information sharing between the private and public sectors.

An example of effective collaboration in this area is an initiative such as the **Financial Services Information Sharing and Analysis Center (FS-ISAC)**. FS-ISAC shares indicators of threats, vulnerabilities and incidents. A group of analysts validates the threat information and sends it to members. As a method of communication, FS-ISAC uses an automated threat intelligence platform, the Traffic Light Protocol (TLP). This platform limits the dissemination of confidential or sensitive information to appropriate audiences based on its sensitivity and source.[16]

The objective of the **National Cyber-Forensics and Training Alliance (NCFTA)**, also in the United States, is to identify, mitigate and disrupt cybercrime through international collaboration[17] between private industry, academia and law enforcement. The NCFTA encourages the prompt sharing of information on major cyber threats to business interests and emerging cyber threat trends. Its work has resulted in hundreds of criminal investigations and charges laid against more than 300 cybercriminals worldwide. The NCFTA has also produced more than 500 intelligence reports on cyber threats over the past 3 years alone.[17] The success of this partnership lies in the ability to provide not-for-profit, non-governmental collaboration that governments can call on when permitted and protect the data chain of custody that could be used in future online criminal prosecutions. Similar cross-sectoral models are needed for effective data sharing.[17]

In the United Kingdom, **Cifas** is a not-for-profit fraud prevention service that brings together private, public and volunteer sector organizations.[18] Cifas is overseen by a board of directors that sets strategic directions and objectives, measures performance against strategic objectives and reviews risks and controls. The organization manages two of the largest fraud prevention databases in the UK: the National Fraud Database and the Internal Fraud Database. This partnership creates a non-competitive, collaborative fraud prevention environment.

In Australia, the **Fintel Alliance, set up by the Australian Transaction Reports and Analysis Centre (AUSTRAC)**, seeks to combat money laundering and terrorist financing.[19] It includes 22 public and private sector organizations and is recognized as the first public-private partnership of its kind. Established in March 2017, it helps private-sector members identify and report suspicious transactions and law enforcement members arrest and prosecute criminals and work with the university community to develop knowledge. Members provide information to Fintel Alliance through AUSTRAC (the hub), which disseminates it to other members on a secure, controlled platform. Members may not share information directly with other member organizations unless doing so is legally permissible.[19] The PPP also has an innovation hub that acts as a kind of "creative sandbox." This allows partners to jointly design new financial products, services and systems that could enhance the intelligence detection and analysis capabilities of the operations centre. One of the significant benefits is the potential to reduce the sector's regulatory burden.[19]

In Canada, the **Canadian Cyber Threat Exchange (CCTX)**, established in 2015, helps businesses and clients protect themselves from cyber threats. To date, the CCTX includes nearly 130 telecommunications firms, financial institutions, insurance and transportation companies, and other organizations.[20] Members can submit data in structured or unstructured format through a web portal.[20] The organization uses STIX and TAXII protocols to characterize data and electronically transfer data between members to reduce human intervention.[20] A key aspect of data sharing among CCTX members is that data is anonymized, meaning that an organization receiving the information will not be able to identify the organization providing it.[20]

Recommendations

The issues and success factors of effective collaboration must be considered. In addition, both the private and public sectors need incentives and motivation to share information to address cultural and reputational obstacles.[9] Reciprocity is also required; information and intelligence must be shared in both directions. To that end, a new security framework for the protection of critical infrastructure must be put in place.[3]

Critical infrastructure protection involves numerous stakeholders. This makes it difficult to identify the responsibilities of each player within a partnership, since current governance systems do not take this plurality into account. A new security framework should be developed to address both private and public sector concerns and interests.[3] Specifically, it should ensure that critical infrastructure companies of all sizes can protect themselves from cyber threats. Measures must therefore be developed thoughtfully to avoid reactive measures being taken in the future.[11] This framework must also be flexible and include a

bottom-up approach so that complex cyber threats can be dealt with in the future.[20] An industry-led public-private partnership approach will ensure that measures are effective and benefit from government resources.

The public sector plays a key role in regulating the structure and setting the rules to be followed in PPP development. Adopting new legislation and developing coordinated procedures would increase stakeholders' understanding and enable them to deal with cyber threats more effectively. In addition, technical communications standards, such as STIX and TAXII, should be used to automate the sharing of cybercrime data and cybersecurity threat indicators in real-time. Lastly, given the rapidly evolving nature and international scope of cyber threats, PPPs should focus on increasing resilience in the financial sector.

Study limitations

To date, there is still too little literature on how an effective PPP should be structured and governed. Legal challenges, privacy, and reputation risks are the biggest obstacles to effective collaboration in a public-private partnership. However, there is no consensus on how to improve this collaboration.[21] The main conclusions drawn from the literature are that the concept of information sharing and the legal framework are still relatively vague. Consequently, it is imperative to continue the research and, more specifically, to clarify aspects of the structure of PPPs that involve financial institutions.

References

[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.