

Canadian
Forces
College

Collège
des
Forces
Canadiennes



THE VALUE OF INTELLIGENCE SHARING FOR CANADA: THE FIVE EYES CASE

Major Sylvain Rouleau

JCSP 46

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2020.

PCEMI 46

Solo Flight

Avertissement

Les opinions exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2020.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46

2019 - 2020

SOLO FLIGHT

THE VALUE OF INTELLIGENCE SHARING FOR CANADA: THE FIVE EYES CASE

By Major Sylvain Rouleau

“This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

Word Count: 5,120

“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”

Nombre de mots : 5.120

THE VALUE OF INTELLIGENCE SHARING FOR CANADA: THE FIVE EYES CASE

INTRODUCTION

The intelligence world, by its very nature, remains relatively secretive and limited studies exist with regard to the value of intelligence sharing for a nation like Canada. That said, the fact that Canada is actively involved in the exchange of classified information with multiple international partners is now in the public domain. The latest Canadian defence policy states that “Canada will continue to foster and strengthen intelligence sharing relationships in a spirit of reciprocity [with the Five Eyes network of partners and other allies].”¹ In this context, what are the costs and benefits of Canada’s reciprocal intelligence sharing with the Five Eyes community comprised of Canada, the United States (US), the United Kingdom (UK), Australia and New Zealand?² Answering this question will help identify the way forward with regard to this unique alliance as well as the challenges and value it brings to Canadians.

Generally speaking, within the Five Eyes context, Canada is deemed to be a junior partner and a net recipient of intelligence products.³ From a rational perspective, this suggests that the overall benefits of the sharing agreement exceed the costs. Therefore, Canada should aim at maintaining and reinforcing the arrangements that currently exist with the Five Eyes partners. However, by following this path, Canada will face enduring cooperation challenges and will remain mostly dependent on the US intelligence apparatus and overarching policies in order to build its own, comprehensive

¹ Department of National Defence, *Strong, Secured, Engaged: Canada’s Defence Policy* (Ottawa: Minister of National Defence, 2017), 65.

² *Ibid.*, 64.

³ Andrew O’Neil, “Australia and the ‘Fives Eyes’ Intelligence Network: The Perils of an Asymmetric Alliance,” *Australian Journal of International Affairs* 71, no. 5 (2017): 537.

global situation awareness.⁴ There is a cost associated with that in terms of national autonomy, but this course of action, as it will be demonstrated, is rooted in deep historical ties and should be understood as a deliberate national decision based on alignment with the US and other like-minded nations in a competitive, multipolar world. Consequently, this paper suggests that it is in the strategic interest of Canada to maximise its national security through a continued and enhanced participation in the Five Eyes network. Meanwhile, Canada and its partners should address existing intelligence collaboration challenges with innovative policies based on transparency and best practices.

To answer the overarching question of the costs and benefits of the Canadian participation in the Five Eyes community, the core of this paper will be divided in three sections. The first section will trace the history of intelligence collaboration between Western nations during the 20th century and explore the challenges of intelligence sharing today with respect to security, privacy and accountability. The second section, based on available unclassified sources, will further elaborate on the genesis of the Five Eyes network and describe the current state of affairs within this community of interest in order to evaluate the pros and cons of the alliance for Canada. Finally, the third section will propose a way forward for Canada's intelligence sharing with its Five Eyes partners.

THE CHALLENGES OF INTELLIGENCE SHARING

Intelligence dissemination questions are nothing new. Rose Mary Sheldon, Roman Empire specialist and Professor at the Virginia Military Institute, mentions that "Targeting an enemy and collecting intelligence must go hand in hand with the ability to transmit the information to those who need it most. One of the Roman Army's basic

⁴ *Ibid.*, 529.

needs, therefore, was the ability to transmit intelligence.”⁵ She further demonstrates that the Romans were involved in quite a variety of intelligence activities covering both the political and military realms.⁶ She concludes that the ability to access intelligence was already instrumental to the political decision-making process in ancient Rome.⁷ One thousand years later, the Byzantine Empire, which had been the world’s greatest power for centuries at that point, proved with the Battle of Manzikert that even the most powerful nation of an era can be permanently defeated if leaders misread their strategic circumstances and miss or ignore imminent dangers.⁸ Another thousand years later, at the time of World War II (WWII), not much had changed with regard to the strategic value of intelligence, but the imperative to share it among specialists and funnel it to decision-makers was no longer limited to single empires or nation-states.

In 1976, after WWII documents started to be declassified, journalist William Stevenson published a captivating book on the covert war that took place during the conflict. In *A Man Called Intrepid: The Secret War 1939-1945*, Stevenson tells the story of a very successful intelligence hub known as British Security Coordination (BSC).⁹ BSC, as early as 1940, was involved in intelligence collaboration between Britain and America in response to the threats posed by Nazi Germany, Imperial Japan and Fascist Italy.¹⁰ The secret entity headquartered in New York was headed by Canadian Sir William Stephenson – also known as Intrepid – who was tasked with the establishment of

⁵ Rose Mary Sheldon. *Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify* (New York: Frank Cass, 2005) 199.

⁶ *Ibid.*, 5.

⁷ *Ibid.*, 276.

⁸ Jai Galliot and Warren Reid, “Introduction,” in *Ethics and the Future of Spying*, ed. Jai Galliot and Warren Reid (New York: Routledge, 2016), 1-2.

⁹ William Stevenson, *A Man Called Intrepid: The Secret War 1939-1945* (London: MacMillan, 1976).

¹⁰ *Ibid.*, xi-xii.

intelligence liaison between Churchill and Roosevelt months before the US was officially at war.¹¹ Ultimately, through the exchange of top secret signals intelligence (SIGINT) derived from the decryption of enemy messages, such intelligence cooperation critically enabled the Allied victory by making, among many other things, the D-Day deception plan possible and credible.¹²

In hindsight, by uniting the key players of the Anglosphere through high-level intelligence sharing in a time of unprecedented global uncertainty, the collaboration effort between BSC and its US counterpart (eventually known as the Office of Strategic Services, the wartime predecessor of the Central Intelligence Agency created in 1947) appears to be the linchpin behind what would later become the Five Eyes network.¹³ This collaboration effort also marked the beginning of a wider trend of intelligence sharing between nations of the Western world throughout the Cold War and beyond. The North Atlantic Treaty Organization (NATO), the North American Aerospace Defence Command (NORAD) and the European Union (EU), for example, all developed intelligence sharing frameworks between their members over the years, so too has the US with numerous bilateral or multilateral partners across the world.¹⁴

Despite this trend, however, intelligence sharing beyond one's own national enterprise, either through a bilateral or a multilateral agreement, can be challenging for different reasons. The heightened collaboration between states and organisations has, in fact, accentuated the perils and difficulties of intelligence cooperation. The obvious

¹¹ *Ibid.*

¹² *Ibid.*, 461-462.

¹³ *Ibid.*, 466.

¹⁴ Craig Forcece, "The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing," in *International Intelligence Cooperation and Accountability*, ed. Hans Born, Ian Leigh, and Aidan Wills (New York: Routledge, 2011), 73-76.

precondition of collaboration is trust between partners. Political Science Professor Andrew O’Neil from Griffith University captures this reality with the following statement: “The formation of alliances, how they operate over time and whether they can be sustained over the long term are all contingent on a range of factors. In particular, the perceived reliability of security guarantees and assurances is central to alliances”¹⁵ That said, trust between allies is not immutable. The appetite for sharing and the national policies of partners involved in transnational intelligence collaboration can be challenged, as demonstrated through a growing body of literature, with concerns over security, privacy and accountability.¹⁶ Through the lens of recent history, our focus will now turn to these three aspects of intelligence sharing in order to inform the forthcoming analysis of the Five Eyes membership value for Canada.

According to retired Canadian Brigadier-General and national security expert James Cox, “Canadians remain generally unaware of the extent to which Canada’s national security relies on Five Eyes intelligence.”¹⁷ As such, the true consequences of the arrest, in January 2012, of Canadian Sub-Lieutenant Jeffery Delisle for supplying top secret intelligence to Russia were difficult to assess at the time by media commentators and the Canadian public.¹⁸ Nonetheless, with this event, it became more obvious for Canadians in general that cases of espionage, such as this one, have the potential to damage both the reputation of Canada and its ability to collaborate with international intelligence partners. Therefore, Cox concludes that “Canada must work to restore the

¹⁵ O’Neil, “Australia and the ‘Fives Eyes’ Intelligence Network”, 531.

¹⁶ See upcoming notes and bibliography for specific references addressing each element.

¹⁷ James Cox, *Canada and the Five Eyes Intelligence Community*, Strategic Studies Working Group Papers, Canadian International Council and Canadian Defence & Foreign Affairs Institute (Calgary: CDFAI & CIC, December 2012): 4.

¹⁸ *Ibid.*

trust and confidence of its Five Eyes partners”¹⁹ This leads to our first conclusion pertaining to information and intelligence security: a single breach by a partner within an alliance can potentially compromise years of successful collaboration and put the pre-existing level of trust between members of the partnership to the test.

The flip side of this conclusion is that member nations of an intelligence sharing alliance can also be confronted with the consequences of security breaches or leaks occurring elsewhere within the network. From a governmental perspective, the revelation, by any actor within a collaborative secret network, of sensitive information that was not originally intended for public disclosure can compromise existing or prospective programmes and policies, expose sources, operations or vulnerabilities, and may even lead to national embarrassment.²⁰ As of 2020, the names of Julian Assange, Chelsea Manning and Edward Snowden, all associated with the voluntary release of US and Five Eyes classified documents through outlets such as WikiLeaks, are well known in the public sphere.²¹ While the specific content and accuracy of the revelations is beyond the scope of this paper, assessing their impact still appears relevant. For example, CBC journalist Peter Zimonjic highlights how WikiLeaks documents exposed the fact that Canada allegedly offered help to invade Iraq in 2003 while publicly defending a diametrically opposed position.²²

¹⁹ *Ibid.*, 9.

²⁰ Warren E. Snyder, “Leaks and Their Consequences: A Guide to the Controversy Over Secrecy vs. Open Government,” *American Intelligence Journal* 32, no. 2 (2015): 13-14.

²¹ Michael R. Touchton *et al.*, “Whistleblowing or Leaking? Public Opinion toward Assange, Manning, and Snowden,” *Research and Politics* 7, no.1 (January-March 2020): 1.

²² Peter Zimonjic, “9 Canadian Stories WikiLeaks Helped Bring to Light,” *CBC News*, last modified 12 April 2019, <https://www.cbc.ca/news/politics/9-canadian-stories-wikileaks-helped-bring-to-light-1.5094640>.

From the example above, we can draw a second conclusion pertaining to information and intelligence security in the context of a multinational collaboration framework: security breaches, leaks and other forms of unplanned disclosures can occur and most likely will at some point. When such is the case, no matter how and where within the network the disclosure takes place, the consequences from a national perspective can be significant in terms of intelligence operational effectiveness and overall credibility.²³ It follows that the risk of unintended classified information disclosure, which can potentially be damaging to the national interest of one or more of the countries participating in the cooperation effort, must be carefully weighed against the perceived benefits of the alliance. Arguably, from a statistical point of view, the larger the alliance, the greater the risk of leakage, but the qualitative nature of a leak appears to be more important than the quantity of occurrences in the grand scheme of things. In any case, the consequences of unplanned disclosures can be far-reaching, sometimes leading to policy or public debates, as in the cases where privacy and accountability questions are raised.

According to former intelligence analyst Patrick Walsh and professorial research fellow Seumas Miller, “The tension between the legitimate collection of information for national security and the rights to privacy of the individual in liberal democratic states has increased markedly since 9/11.”²⁴ In the years following this attack on US soil, the Five Eyes members all implemented reform measures giving their respective intelligence agencies “far greater surveillance and collection capabilities to proactively detect, disrupt

²³ Snyder, “Leaks and Their Consequences . . .”, 16.

²⁴ Patrick F. Walsh and Seumas Miller, “Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practices Post Snowden,” *Intelligence and National Security* 31, no. 3 (2016): 345.

and arrest difficult to get at non-state threats like terrorism and transnational criminals that they had pre-9/11.”²⁵ While such an approach can be justified by governments to promote national and transnational security interests, it also has the potential to erode aspects of domestic sovereignty, the concept referring to the ability of states to control and regulate activities within their territories.²⁶ Specifically, junior partners within an alliance may be limited in their ability to protect the privacy of their own citizens if the information flows that are of interest to the alliance are transnational in nature or if the group’s policy orientations are dictated, or at least heavily influenced, by its most powerful stakeholder.

Craig Forcese, Professor of Law at the University of Ottawa, states the following with regard to the privacy considerations linked to intelligence collaboration activities: “Intelligence sharing engages . . . two important dimensions of privacy protection: the impact of global intercept capacity in a world in which privacy is regulated nationally and the . . . consequences of migration of private information across international borders.”²⁷ If we juxtapose these privacy considerations with the conclusions by Walsh and Miller that (1) the post-9/11 reforms within the non-US Five Eyes nations were basically a reflection of the US ones in order to ensure continued collaboration, and (2) the Snowden revelations about the Five Eyes agencies’ global collection capabilities (e.g. wiretaps, metadata, social media, etc.) represent, by definition, an infringement of the right to privacy, then we can draw a new conclusion.²⁸ This conclusion is that intelligence

²⁵ *Ibid.*, 346.

²⁶ Stephen D. Kasner, “The Persistence of State Sovereignty,” in *International Politics and Institutions in Time*, ed. Orfeo Fioretos (Oxford: Oxford University Press, 2017), 41.

²⁷ Forcese, “The Collateral Casualties of Collaboration . . .”, 79.

²⁸ Walsh and Miller, “Rethinking ‘Five Eyes’ Security Intelligence . . .”, 345-346, 350.

sharing between nations can lead, either by design or indirectly, to a limitation of the privacy rights of citizens within the member nations, especially junior members with limited agenda-setting privileges. Once again, being part of the club has a cost in terms of autonomy and the utility of this national sovereignty ‘sacrifice’ should be assessed against the overall benefits produced by the alliance.

Finally, a third aspect of transnational intelligence sharing that raises concerns is the question of accountability. As with the privacy issue, these concerns are the result of an apparent disconnect between national and international responsibilities and obligations. Professor of Law Ian Leigh from Durham University explains that, since 9/11, “certain manifestations of intelligence cooperation have led to high-profile controversies, such as the revelations about the extraordinary rendition, interrogation and secret detention of suspected terrorists.”²⁹ However, he adds, “International cooperation has in general evaded the scrutiny of national oversight and review structures, which were designed for a different era and in response to a very different set of abuses.”³⁰ In other words, there is a perceived accountability gap at the national level with regard to intelligence activities occurring at the international level. Furthermore, the increasing trend of intelligence cooperation between nations in the last few decades has not been matched by a similar level of collaboration between national oversight and review bodies, which means that the accountability gap also has a transnational component.³¹

²⁹ Ian Leigh, “Accountability and Intelligence Cooperation: Framing the Issue,” in *International Intelligence Cooperation and Accountability*, ed. Hans Born, Ian Leigh, and Aidan Wills (New York: Routledge, 2011), 3-4.

³⁰ *Ibid.*, 4.

³¹ *Ibid.*

Within the Canadian context, the topic of accountability in matters pertaining to national security has been studied for some time now. Professors Reg Whitaker and Stuart Farson, respectively from York and Simon Fraser University, were already exploring this subject over 10 years ago and proposing different avenues in order to increase the level of accountability imposed on security and intelligence agencies in Canada.³² One of their primary recommendations, the creation of a committee of Parliament for national security, was eventually followed by the Government of Canada with the establishment of the National Security and Intelligence Committee of Parliamentarians in 2017. This committee, which is comprised of members from both chambers holding top secret security clearances, has an extensive review mandate with respect to any matter relating to national security and intelligence in terms of policy, finance, administration or operations.³³

That being said, even proponents of a robust national intelligence accountability framework, such as Whitaker and Farson, recognize the necessity for secrecy in dealing with national security questions. “The various organizations making up Canada’s security and intelligence community have special and necessary requirements for secrecy that exceed the requirements for secrecy in other areas of government operations.”³⁴ A major reason for such a level of concealment is the reliance by Canada on information received in confidence from foreign governments and vice-versa.³⁵ Therefore, even with a strong national accountability framework, the two-way imperative for secrecy that is implicit to

³² Reg Whitaker and Stuart Farson, “Accountability in and for National Security,” *IRPP Choices* 15, no. 9 (2009): 40-42.

³³ National Security and Intelligence Committee of Parliamentarians, “About: Mandate,” last accessed 1 May 2020, <https://www.nsicop-cpsnr.ca/index-en.html>.

³⁴ Whitaker and Farson, “Accountability in and for National Security,” 8.

³⁵ *Ibid.*, 9.

any intelligence sharing agreement may lead to some forms of accountability deficits at the supranational level. As such, the conclusion drawn from the accountability problem developed above is that intelligence sharing between international partners offers limited control over the use, by the other partners, of the information provided in confidence to the network, and thus no real assurance of accountability above the national level.

THE FIVE EYES INTELLIGENCE NETWORK

Having traced the modern history of intelligence collaboration between Western nations back to the middle of the last century and framed the current problematic of intelligence sharing around security, privacy and accountability issues, we will now focus on the specificities of the Five Eyes network. Many terms and expressions have been employed over the years to describe this exclusive club which relies on a series of agreements and procedures between its members for its operations, but which is not a formal treaty organization such as NATO.³⁶ While Miller and Walsh describe the Five Eyes as an espionage and cyber-espionage alliance, others evoke, with a more critical tone, a system of secret and pervasive surveillance inflicted upon the world by the US government and its ‘client states.’³⁷ Noting the difference in connotation by different authors in describing the Five Eyes partnership, a factual recollection of the network’s genesis and a comprehensive description of its functions and features appear essential to the discussion at this stage.

³⁶ O’Neil, “Australia and the ‘Fives Eyes’ Intelligence Network . . .”, 530-531.

³⁷ Seumas Miller and Patrick Walsh, “The NSA Leaks, Edward Snowden, and the Ethics and Accountability of Intelligence Collection,” in *Ethics and the Future of Spying*, ed. Jai Galliot and Warren Reed (New York: Routledge, 2016), 202; Jeremy Wisniewski, “WikiLeaks and Whistleblowing,” in *Ethics and the Future of Spying*, ed. Jai Galliot and Warren Reed (New York: Routledge, 2016), 213.

According to O’Neil, “The Five Eyes network is the world’s oldest formalised intelligence network and has its origins in the significant expansion of Allied intelligence cooperation and exchange during World War II.”³⁸ This cooperation has been particularly evident in the SIGINT domain.³⁹ Also, based on its endurance over time, the Five Eyes network has become central in shaping the conceptualization of intelligence cooperation in academia over the past decades.⁴⁰ Yet, public knowledge about the arrangements behind this partnership and the nature of the collaboration between its partners remains limited. This can be explained by the fact that the current level of transparency among governments with respect to the Five Eyes is a relatively new phenomenon.⁴¹ Based on the research conducted by University of Sydney scholars Felicity Ruby, Gerard Goggin and John Keane, the first-ever open acknowledgment of the existence of the Five Eyes came from Australia in 1999 when Martin Brady, then director of the Defence Signals Directorate, stated on television that his organization was cooperating with SIGINT counterparts overseas under the UKUSA relationship.⁴²

This so-called UKUSA relationship is key to understand the Five Eyes connection that exists today. Jeffrey Richelson, a senior fellow at the National Security Archive in Washington, explains the genesis of the UKUSA Agreement as a series of wartime SIGINT cooperation initiatives that were successively developed from 1940 onward between the US and the UK (including the British Dominions) and which were ultimately

³⁸ O’Neil, “Australia and the ‘Fives Eyes’ Intelligence Network . . .”, 533.

³⁹ *Ibid.*

⁴⁰ Zakia Shiraz and Richard J. Aldrich, “Secrecy, Spies and the Global South: Intelligence Studies Beyond the ‘Fives Eyes’ Alliance.” *International Affairs* 95, no. 6 (2019): 1313-1314.

⁴¹ Felicity Ruby, Gerard Goggin, and John Keane, “‘Comparative Silence’ Still? Journalism, Academia, and the Five Eyes of Edward Snowden,” *Digital Journalism* 5, no. 3 (2017): 355.

⁴² *Ibid.*, 356.

formalized under a unique umbrella in 1954.⁴³ “The Primary emphasis of the agreement was to provide a division of SIGINT collection responsibilities between the First Party (the United States) and the Second Parties (Australia, Britain, Canada, and New Zealand).”⁴⁴ Under this enduring division of responsibilities resulting from the agreement, the Five Eyes partners each have their respective SIGINT mandates to cover a portion of the world for the benefit of the entire community. The US is responsible for Russia, northern China, most of Asia and Latin America. Australia covers southern China, the nations of Indochina and its close neighbors, such as Indonesia. The UK is in charge of SIGINT collection in Africa and west of the Urals within the former Soviet Union. And, finally, New Zealand is responsible for the Western Pacific while Canada is responsible for the polar regions of Russia.⁴⁵

Throughout its existence, however, the Five Eyes relationship has become “more than an agreement to coordinate separately conducted intelligence activities and share the intelligence collected.”⁴⁶ The relationship has been cemented by the presence of US facilities in the UK, Australia and Canada, by joint operations across the world and by staff exchanges. Furthermore, over the years, the agreement has led to the creation of common indoctrination procedures for intelligence producers and users, strict information access protocols, and comprehensive data handling security arrangements which all exemplify professional best practices in the field of intelligence.⁴⁷ In addition to that, through a series of collaborative endeavors over the past 60 years, and to this day, the

⁴³ Jeffrey T. Richelson, *The US Intelligence Community*, 6th ed. (Boulder: Westview Press, 2012), 348-349.

⁴⁴ *Ibid.*, 349.

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*, 350.

⁴⁷ *Ibid.*

Five Eyes partners have become collectively involved in ocean and maritime surveillance, scientific and defence intelligence analysis, medical intelligence, geospatial intelligence, counterintelligence, counterterrorism, and, last but not least, the continuous sharing of intelligence products via a collective database at the top secret level known as STONE GHOST.⁴⁸

The last point from the list above is quite important is assessing the value of the Five Eyes for Canada. The existence of such a system where members of the intelligence community can execute searches within a highly classified setting and access products derived from the collection and processing capabilities of the entire network represents an extremely valuable asset in itself. The database also proves that the Five Eyes partners have achieved a very high level of interoperability over time. The Office of the Director of National Intelligence offers this perspective on intelligence collaboration: “A considerable hurdle in information sharing is establishing trust and interoperability among the two or more organizations that want to share information.”⁴⁹ Prior to sharing intelligence, organizations look for assurances that all the partners with whom they wish to share are implementing policies and standards in a manner worthy of trust.⁵⁰ Therefore, the continued access to the Five Eyes systems and databases (which is assumed based on the 2017 Canadian defence policy) proves that Canada, despite the Delisle case, has remained trustworthy among the Five Eyes and can thus access a vast amount of intelligence products, more than it could ever realistically produce nationally.

⁴⁸ *Ibid.*, 351-352.

⁴⁹ Office of the Director of National Intelligence, “Establishing Trust and Interoperability in the Information Sharing Environment,” last accessed 3 May 2020, <https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/ise-archive/ise-mission-stories/1824-establishing-trust-and-interoperability-in-the-information-sharing-environment>.

⁵⁰ *Ibid.*

In terms of burden sharing, the Five Eyes network is undeniably asymmetric. From a transactional perspective, both the collection capacity and production throughput ratios between the First Party and the Second Parties, also known as junior partners, clearly favor the latter.⁵¹ As Political Science Professor Loch Johnson points out, “the US continues to have the largest and most expensive intelligence apparatus in the world, indeed in the history of humankind.”⁵² As a consequence, the US inputs much more data into the network than any other counterpart. Therefore, if we consider the claim by Cox that the Five Eyes network is instrumental in feeding and shaping the Canadian national assessments produced by the Intelligence Assessment Secretariat of the Privy Council Office and by the Chief of Defence Intelligence, then we have to conclude that, under the current circumstances, Canada is to a great extent dependent on the US intelligence apparatus in order to build its own national situational awareness and inform decision-makers on global intelligence matters.⁵³

Such an imbalance between intelligence sharing partners is not unusual. Political Science Professor James Walsh from Charlotte explains that this is often happening by design as governments seeking to share intelligence create hierarchical relationships to manage risks, monitor compliance and facilitate the overall decision-making process within the alliance.⁵⁴ “Governments agree to create and to enter such hierarchies, even when they infringe on national decision making autonomy, because they are a reliable way to mitigate concerns about defection and to engage in mutually beneficial

⁵¹ O’Neil, “Australia and the ‘Fives Eyes’ Intelligence Network . . .”, 529.

⁵² Loch K. Johnson, “The United States,” in *PSI Handbook of Global Security and Intelligence: National Approaches, Volume 1: The Americas and Asia*, ed. Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro (Westport: Praeger, 2008), 64.

⁵³ Cox, *Canada and the Five Eyes Intelligence Community . . .*, 7-9.

⁵⁴ James I. Walsh, “Defection and Hierarchy in International Intelligence Sharing,” *Journal of Public Policy* 27, no. 2 (2007): 152.

cooperation.”⁵⁵ For recipients such as Canada, the principal benefit is the acquisition of intelligence that is valuable to decision-makers but impossible to obtain otherwise at an acceptable cost.⁵⁶ The dominant player, the US in this case, also benefits from the partnership by selecting its partners, determining the policy orientations of the coalition, extending its global reach, and accessing a wider pool of intelligence specialists and analysts.⁵⁷ In summary, while asymmetric in nature, the Five Eyes network represents a long-standing and very beneficial partnership for Canada and the other junior partners as it contributes greatly to their respective national security enterprises. However, this relationship implies a partial relinquishment of national autonomy.

THE WAY FORWARD FOR CANADA

Within the security studies liberalist paradigm, the idea of parting with elements of sovereignty can sometimes be justified. If a form of cooperation between states is deemed important enough, the national interest may transcend autonomy and sovereignty, leading nations to redefine their interests in order to embrace the necessary reduction in independence required by the cooperation effort.⁵⁸ With regards to Canada’s Five Eyes membership, this model explains the continued resolve of the government to engage in collaboration with the like-minded nations that form the Anglosphere. After all, this relationship dates back to the 1940s and has been very successful over time, starting with the Allied victory during WWII, which was partly enabled by collaborative SIGINT work, and continuing to this day with uninterrupted trends of intelligence cooperation in

⁵⁵ *Ibid.*

⁵⁶ *Ibid.*, 157.

⁵⁷ Richelson, *The US Intelligence Community* . . . , 347-356.

⁵⁸ Patrick Morgan, “Liberalism,” in *Contemporary Security Studies*, 5th ed., ed. Alan Collins (Oxford: Oxford University Press, 2019), 35.

multiple areas of expertise.⁵⁹ Put differently, the Five Eyes relationship brings tremendous benefits to Canada in comparison to the small cost paid in terms of reduced national autonomy. It is therefore in Canada's strategic interest to maintain and reinforce the Five Eyes partnership. Nevertheless, the challenges of intelligence collaboration previously highlighted with regards to security, privacy and accountability must be addressed in order to inform the way forward for Canada and its Five Eyes partners.

The security question could very well represent the first obstacle for Canada on the road to enhanced collaboration with the other Five Eyes nations. As demonstrated previously, a single security breach emanating from Canada can jeopardize the level of trust granted by partners. Fortunately, the Delisle case from 2012 has had minimal impact over time, but another case, arguably much more problematic, has recently surfaced in the media. In September 2019, Cameron Otis, the director general of the national intelligence co-ordination center of the Royal Canadian Mounted Police (RCMP) was arrested under charges pertaining to the communication or confirmation of special operational information to unauthorized parties.⁶⁰ CBC journalist Catharine Tunney reports having accessed the following damage assessment originating from the Communications Security Establishment (CSE): "CSE's preliminary assessment is that damage caused by the release of these reports and intelligence is HIGH and potentially devastating in that it would cause grave injury to Canada's national interests."⁶¹

⁵⁹ Stevenson, *A Man Called Intrepid: The Secret War 1939-1945*, 461-462; Richelson, *The US Intelligence Community* . . . , 350-352.

⁶⁰ Catharine Tunney, "Intelligence Community Reeling after RCMP Director Accused of Violating Secrets Act," *CBC News*, last modified 18 September 2019, <https://www.cbc.ca/news/politics/rcmp-security-charge-1.5280643>.

⁶¹ Catharine Tunney, "RCMP Head Says Allies Concerned, But Supportive in Wake of Spy Charges," *CBC News*, last modified 17 September 2019, <https://www.cbc.ca/news/politics/rcmp-cameron-ortis-update-1.5286563>.

As the demarcation lines between criminal and security investigations as well as between foreign and domestic intelligence got blurred since 9/11, more Canadian agencies have become regularly involved in intelligence sharing with the Five Eyes, including the RCMP and the Canadian Security Intelligence Service (CSIS).⁶² This is consistent with the widening of the Five Eyes mandate over time from a defence-focused, SIGINT-only organization to a comprehensive, all-source intelligence sharing network. As a consequence, many agencies could be affected by a restriction on information exchange imposed on Canada by partner nations. As such, the Canadian government must thoroughly investigate the Otis case, find mitigation measures to ensure security breaches at such a high level do not occur again, and provide assurances to the Five Eyes partners that the security procedures and security clearance measures in place remain adequate. Failure to do so will compromise the long-term Canadian access to the Five Eyes network and negatively affect national security interests.

As per the second collaboration security challenge identified previously, the risk of unintended information disclosure occurring elsewhere in the network with a detrimental effect on Canada, transparency appears to be the most viable strategy considering that leaks will likely continue to occur from time to time. In order to avoid credibility deficits, conspiracy theories or even national embarrassment, Canada and the other Five Eyes governments must continue to engage in open practices with respect to the divulgence of their collaborative intelligence arrangements and programmes. This is not to say that the secrecy surrounding the work of intelligence professionals must be abandoned altogether, not at all. Rather, this is a recognition of the reasonable

⁶² Forcese, “The Collateral Casualties of Collaboration . . .”, 74.

expectations by citizens of democratic states to be informed about the machinery behind the collective good of national security.⁶³ Actually, the open acknowledgment of the Five Eyes network's existence over the past 20 years by the different governments of the participating nations definitely represents a step in the right direction. This kind of initiatives which balance security imperatives with open disclosure practices must continue through measured, but significant transparency efforts.

The challenge of privacy is more difficult to resolve. Striking the perfect balance between privacy and security is a recurring problem in democratic societies and a wicked one too as there is no easy solution to satisfy both imperatives at the same time. The reality is that the continued involvement of Canada with the Five Eyes has the potential, in certain circumstances, to affect the privacy rights of Canadian citizens. This is especially true since Canada has limited influence on the policy orientations of the alliance and must sometimes accept certain practices dictated by the US in order to ensure interoperability and maintain the relationship.⁶⁴ Having said that, a 'pre-emptive disclosure' approach based on transparency could, once again, mitigate the negative consequences of the privacy limitations imposed on Canadians by the Five Eyes membership. At least, it would inform the population on the collective price to pay in order to be a member of the most successful intelligence partnership in history.

With regards to intelligence accountability, all the Five Eyes partners are subjected to oversight and review bodies at the national level. As noted in a research paper produced by the Library of Parliament, each of the five countries has developed "a

⁶³ Mark Jensen, "The Virtues of Bond and Vices of Bauer: An Aristotelian Defence of Espionage," in *Ethics and the Future of Spying* (New York: Routledge, 2016), 15.

⁶⁴ Walsh and Miller, "Rethinking 'Five Eyes' Security Intelligence . . .", 345-346.

framework that includes a system of checks and balances that spans the various branches of government, and which aims to ensure that agencies are accountable for both their administration and expenditure and the legality and propriety of their activities.”⁶⁵ Now, in order to tackle the transnational accountability gap previously underlined, the next step forward to achieve a more complete form of accountability would be the formal networking of the different Five Eyes review bodies. To that effect, Leigh suggests that “oversight bodies may attempt to mirror the behaviour of the agency they oversee and engage in networking. . . . This could take place through joint committees, sharing of information or the creation of supranational bodies.”⁶⁶ While the specific approach to follow should be discussed by governments, such an idea demonstrates that the transnational accountability challenge pertaining to intelligence collaboration is not insurmountable.

CONCLUSION

From the intelligence liaison work of BSC and its Canadian director during WWII to the current shared exploitation of the STONE GHOST database, the Five Eyes partners have demonstrated, over multiple decades, their ability and willingness to work jointly towards collective security for the benefit of their populations and the Western world in general. While Canada contributes to the overall intelligence production of the organization with niche capabilities, such as SIGINT collection in the Arctic, it remains a junior partner and a net recipient of intelligence within the alliance. As such, the benefits of the partnership clearly surpass the costs. Without its membership with the Five Eyes,

⁶⁵ Library of Parliament, “Oversight of Intelligence Agencies: A Comparison of the ‘Five Eyes’ Nations,” *Research Paper Series, 2017-18, ISSN 2203-5249* (Ottawa: Parliament, 2017), 2.

⁶⁶ Leigh, “Accountability and Intelligence Cooperation: Framing the Issue,” 9-10.

Canada would have to expend an extensive amount resources on intelligence gathering to maintain something similar to the current capabilities the nation enjoys. For this reason, this paper suggests that it is in the strategic interest of Canada to maximise its national security through a sustained or even enhanced participation in the Five Eyes network.

By following this path, however, Canada will continue to depend on the US intelligence apparatus in order to produce its own national assessments for domestic decision-makers. This dependence on foreign capabilities certainly has cost in terms of national autonomy, but this cost is deemed to be acceptable when compared to the benefits produced by the alliance such as a wide access to all-source intelligence products. A renewed commitment to the Five Eyes network also has for consequence to trigger the enduring necessity of addressing challenges pertaining to intelligence sharing. Issues of security, privacy and accountability will remain prevalent as Canada maintains a high level of intelligence cooperation with its allies. However, as demonstrated, these issues can be mitigated with best practices, such as review and oversight, and innovative policies based on transparency and open disclosure.

BIBLIOGRAPHY

- Canada. Department of National Defence. *Strong, Secured, Engaged: Canada's Defence Policy*. Ottawa: Minister of National Defence, 2017.
- . Library of Parliament. "Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations." *Research Paper Series, 2017-18, ISSN 2203-5249*. Ottawa: Parliament, 2017.
- . National Security and Intelligence Committee of Parliamentarians. "About: Mandate." Last accessed 1 May 2020. <https://www.nsicop-cpsnr.ca/index-en.html>.
- Cox, James. *Canada and the Five Eyes Intelligence Community*. Strategic Studies Working Group Papers, Canadian International Council and Canadian Defence & Foreign Affairs Institute. Calgary: CDFAI & CIC, December 2012.
- Force, Craig. "The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing." In *International Intelligence Cooperation and Accountability*, edited by Hans Born, Ian Leigh, and Aidan Wills, 72-97. New York: Routledge, 2011.
- Galliot, Jai, and Warren Reid. "Introduction." In *Ethics and the Future of Spying*, edited by Jai Galliot and Warren Reid, 1-12. New York: Routledge, 2016.
- Jensen, Mark. "The Virtues of Bond and Vices of Bauer: An Aristotelian Defence of Espionage." In *Ethics and the Future of Spying*, edited by Jai Galliot and Warren Reid, 15-26. New York: Routledge, 2016.
- Johnson, Loch K. "The United States." In *PSI Handbook of Global Security and Intelligence: National Approaches, Volume 1: The Americas and Asia*, edited by Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro, 52-66. Westport: Praeger, 2008.
- Kasner, Stephen D. "The Persistence of State Sovereignty." In *International Politics and Institutions in Time*, edited by Orfeo Fioretos, 39-55. Oxford: Oxford University Press, 2017.
- Leigh, Ian. "Accountability and Intelligence Cooperation: Framing the Issue." In *International Intelligence Cooperation and Accountability*, edited by Hans Born, Ian Leigh, and Aidan Wills, 3-17. New York: Routledge, 2011.
- Miller, Seumas, and Patrick Walsh. "The NSA Leaks, Edward Snowden, and the Ethics and Accountability of Intelligence Collection." In *Ethics and the Future of Spying*, edited by Jai Galliot and Warren Reed, 193-204. New York: Routledge, 2016.

- Morgan, Patrick. "Liberalism." In *Contemporary Security Studies*, 5th ed., edited by Alan Collins, 30-46. Oxford: Oxford University Press, 2019.
- O'Neil, Andrew. "Australia and the 'Fives Eyes' Intelligence Network: The Perils of an Asymmetric Alliance." *Australian Journal of International Affairs* 71, no. 5 (2017): 529-543.
- Richelson, Jeffrey T. *The US Intelligence Community*. 6th ed. Boulder: Westview Press, 2012.
- Ruby, Felicity, Gerard Goggin, and John Keane. "'Comparative Silence' Still? Journalism, Academia, and the Five Eyes of Edward Snowden." *Digital Journalism* 5, no. 3 (2017): 353-367.
- Sheldon, Rose Mary. *Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify*. New York: Frank Cass, 2005.
- Shiraz, Zakia, and Richard J. Aldrich. "Secrecy, Spies and the Global South: Intelligence Studies Beyond the 'Fives Eyes' Alliance." *International Affairs* 95, no. 6 (2019): 1313-1329.
- Snyder, Warren E. "Leaks and Their Consequences: A Guide to the Controversy Over Secrecy vs. Open Government," *American Intelligence Journal* 32, no. 2 (2015): 13-16.
- Stevenson, William. *A Man Called Intrepid: The Secret War 1939-1945*. London: MacMillan, 1976.
- Touchton, Michael R., Casey A. Klofstad, Jonathan P. West, and Joseph E. Uscinski. "Whistleblowing or Leaking? Public Opinion toward Assange, Manning, and Snowden." *Research and Politics* 7, no.1 (January-March 2020): 1-9.
- Tunney, Catharine. "Intelligence Community Reeling after RCMP Director Accused of Violating Secrets Act." *CBC News*. Last modified 18 September 2019. <https://www.cbc.ca/news/politics/rcmp-security-charge-1.5280643>.
- . "RCMP Head Says Allies Concerned, But Supportive in Wake of Spy Charges." *CBC News*. Last modified 17 September 2019. <https://www.cbc.ca/news/politics/rcmp-ortis-update-1.5286563>.
- United States. Office of the Director of National Intelligence. "Establishing Trust and Interoperability in the Information Sharing Environment." Last accessed 3 May 2020. <https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/ise-archive/ise-mission-stories/1824-establishing-trust-and-interoperability-in-the-information-sharing-environment>.

- Walsh, James I. "Defection and Hierarchy in International Intelligence Sharing." *Journal of Public Policy* 27, no. 2 (2007): 151-181.
- Walsh, Patrick F., and Seumas Miller. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practices Post Snowden." *Intelligence and National Security* 31, no. 3 (2016): 345-368.
- Whitaker, Reg, and Stuart Farson. "Accountability in and for National Security." *IRPP Choices* 15, no. 9 (2009): 1-54.
- Wisnewski, Jeremy. "WikiLeaks and Whistleblowing." In *Ethics and the Future of Spying*, edited by Jai Galliot and Warren Reed, 205-215. New York: Routledge, 2016.
- Zimonjic, Peter. "9 Canadian Stories WikiLeaks Helped Bring to Light." *CBC News*. Last modified 12 April 2019. <https://www.cbc.ca/news/politics/9-canadian-stories-wikileaks-helped-bring-to-light-1.5094640>.