May 2021 – Number 12

# Policy Report

Réseau d'analyse stratégique
Network for Strategic Analysis

## Intelligence Cooperation in a Multipolar World: Non-American Perspectives

**Jonathan Mayne and Marco Munier**

*This policy report follows the conference organized by the Network for Strategic Analysis entitled "Intelligence Cooperation in a Multipolar World: Non-American Perspectives" on May 6, 2021.*

This conference brought together prominent intelligence and strategic studies professionals and academics including: Jill Sinclair of the Department of National Defence, Daniel Jean, former National Security and Intelligence Advisor to the Prime Minister of Canada, Artur Wilczynski of Communications Security Establishment, Heather De Santis from Public Safety Canada, Björn Fägersten from the Swedish Institute of International Affairs, Claudia Hillebrand from Cardiff University, Gustav Gressel from the European Council on Foreign Relations, Adriana Seagle from Bellevue University, Sarah-Myriam Martin-Brûlé from Bishop's University, Stephanie Carvin from Carleton University, Thomas Juneau from the University of Ottawa, Reg Whitaker from Victoria University, Nancy Teeple from the Royal Military College of Canada, Patrick F. Walsh from Charles Sturt University and Justin Massie from the University of Quebec in Montreal.

Although often neglected, intelligence cooperation is not a new phenomenon. In particular, since the emergence of international terrorism, intelligence cooperation has expanded to a global level. This threat continues to pose a challenge to the intelligence services, but the current transition of power and the intensification of strategic competition between the great powers require a shift in the vision of intelligence cooperation.

In this context, the conference aimed to establish a better understanding of the rise of competition between the great powers in a digital world. This phenomenon raises many challenges in a free and open society that requires intelligence cooperation to meet them. Four major themes were addressed during this conference: the challenges of intelligence cooperation, the European Union (EU) as an actor of intelligence, the role of the concept of Intelligence, Surveillance and Reconnaissance on strategic stability, and the future of the Five Eyes, including Canada and Australia, in intelligence cooperation.

Therefore, we can draw from this policy report the lack of international cooperation on subjects of strategic interest at a time of competition between the great powers, such as with new technologies and national reluctance to fully share essential information, except in times of emergencies. This policy report also highlights the lack of accountability and oversight of intelligence sharing activities. However, the fact remains that cooperation continues to grow, and actors like the EU will play an increasingly important role in the world of intelligence and transnational intelligence cooperation. That said, with the significant growth in cooperation needs, many challenges emerge for countries like Canada, which depend on the foreign intelligence capabilities of more powerful allies. In such a case, we must strengthen the capacity

to identify our own threats and national interests, while continuing to cooperate with our allies by providing specific expertise.

Finally, we recommend a "Canadianization" of intelligence for Canada, that is to say to orient the collection and analysis of foreign intelligence towards a clearer and firmer pursuit of specifically Canadian interests, as opposed to the reception of raw or finished intelligence products, which may or may not reflect Canadian needs and interests. In addition to this recommendation are several interesting initiatives, including a more robust and horizontal engagement of the national security and intelligence (NSI) community with non-traditional entities that are now being targeted by emerging threats. Actors such as innovative companies in the field of advanced technologies and centers of research and technological excellence have skills and knowledge available that could enable the NSI community to better respond to emerging threats that require a greater multidisciplinary approach. Supporting the development of knowledge and mitigation strategies in the face of threats would only make external actors more inclined to share more with the NSI community.

## The Challenges of Intelligence Cooperation

Intelligence cooperation, also known as intelligence liaison and intelligence sharing, is one of the most secret intelligence activities and involves many evolving challenges, especially within Western democracies.

First, it should be understood that any intelligence agency operates primarily in its own interests and to support its country's foreign, security, and defence policy objectives. In this context, cooperation occurs when there is a clear benefit outweighing the costs. This is particularly the case to fill a lack of information, to seek different expertise, to reduce the costs of an operation, to fight against a common threat, or to obtain or hope to obtain something in return.

However, there are many constraints, if not restrictions, on intelligence cooperation. Several elements can limit the exchange of information: different perceptions of threats; different national interests; national legal frameworks; organizational cultures; the practices of foreign intelligence agencies, particularly with regard to human rights; or the fear that the information exchanged will be leaked or communicated to a third party, compromising not only the bond of trust, but also the methods and sources of intelligence agencies. This latter concern partly explains why intelligence cooperation is one of the most secret and invisible activities of intelligence agencies and one of the most difficult to map and monitor.

This invisibility of intelligence cooperation will increase as the need for cooperation increases, as has been the case through the fight against terrorism to current Great-power competition. There is then a paradox that forms, between the increase in the invisibility of intelligence activities driven by the increase in cooperation needs, and the desire and the increasingly important need to make intelligence activities democratically responsible and accountable.

Yet today, we find ourselves with an increase in the volume of intelligence exchanged, an increase in the number of actors benefiting from cooperation and growing flexibility in the often ad hoc and temporary arrangements for cooperation. If we add to this the globalization of intelligence cooperation in the era of counterterrorism, then it becomes important to find mechanisms of accountability and oversight of this intelligence activity. While intelligence cooperation is pragmatically useful and necessary, history teaches us that many mistakes, harmful to citizens, have been made by intelligence exchange activities.

However, current accountability and oversight mechanisms are limited by borders and national laws, making it difficult to track intelligence exchanges. We must therefore strengthen these mechanisms, or create supranational accountability and oversight mechanisms, to make the exchange of information more transparent. An intermediary model, not supranational, but institutionalized and transnational, is the Five Eyes Intelligence Oversight and Review Council (FIORC), composed of the main national oversight bodies of the five member countries, and deals with, among other things, how to improve the transparency of intelligence activities.

## The European Union: Intelligence as a Vector of Strategic Autonomy

For many years, the EU, pushed in particular by France and Germany, has been trying to acquire a certain strategic autonomy, that is to say to strengthen its independence, its capacities and its resilience in a number of areas like security and defence, or foreign policy in general. In a multipolar world, characterized by the reappearance of competition between the great powers, certain actors within the EU and certain member states are increasingly motivated to achieve strategic autonomy. On the one hand, to move the EU away from its dependence on the United States for security and defence matters, and on the other, to confront Russian and Chinese ambitions in Europe.

It would seem that one of the vectors for achieving this objective is the creation of a genuine intelligence capacity at the EU level. Indeed, achieving strategic autonomy, that is, having the ability to act according to one's interests, requires understanding the strategic environment. For the EU, the challenge is to define its own threats, without depending on the American threat perceptions.

However, the intelligence capabilities of the EU, like the intelligence cooperation within it, are far from sufficient at present. Besides the need to strengthen the national intelligence capacities of some countries, the very structure of the EU is a challenge for the intelligence services. Based on an area of free movement and free trade, it is often exploited for committing crimes or acts of espionage, and makes the work of national intelligence agencies particularly difficult. The need for cooperation is therefore indispensable. Nonetheless, the exchange of information is still limited, except when a major event occurs.

At European level, there is no supranational body responsible for intelligence. There are, however, bodies facilitating cooperation at the European level, without an intelligence-gathering mandate, but that receive intelligence from EU members' intelligence agencies, such as the Intelligence Analysis Center, the Intelligence Directorate of the EU General Staff or Europol. While intelligence cooperation has been satisfactory in the area of crime and terrorism, the same is not true for the four sectors essential for strategic autonomy, namely decision-making, operational, commercial and technological autonomy. At these levels, intelligence cooperation within the EU is rather rudimentary, given diverging national interests, political will, and perceived threats.

As it is not possible to create a supranational European intelligence agency without changing the treaty, the EU must focus on reinforcing intelligence cooperation between member states through joint training or joint operations to strengthen mutual trust. One example is the Permanent Structured Cooperation (PESCO) project to create a coordination center on cyberspace and information surveillance. Ultimately, creating a real European intelligence capability will require a certain loss of national autonomy and sovereignty.

## The Concept of Intelligence, Surveillance and Reconnaissance: Strategic Opportunity or Vector of Instability?

Intelligence Surveillance and Reconnaissance (ISR) is a strategic concept that enables decision makers to anticipate change, mitigate risk and direct results. It is both an intelligence and an operations activity that synchronizes and integrates the planning and exploitation of sensors, resources, and processing systems to directly support current and future operations. In other words, ISR is an advanced intelligence capability that provides decision-making advantage.

However, the superiority of the United States in this area creates an asymmetry that could call into question strategic stability. Traditionally, strategic stability has been maintained by nuclear deterrence. Today, in the strategic doctrines of the great powers, nuclear power is incorporated with other more traditional capacities. The multiplication of areas of confrontation, particularly space and cyberspace, multidomain deterrence, especially when adversaries like Russia and China use hybrid or gray zone tactics, cyberspace or even new technologies to destabilize Western democracies.

**Superior US intelligence technology capabilities drive increasing reliance by adversaries on asymmetric techniques and operations**

The advantage of the ISR in this complexification of the modes of confrontation is to anticipate the capacities, the intentions and the actions of the adversaries. However, there are certain risks with this strategic advantage, leading to manipulation and disinformation by inferior adversaries at best, and aggressive pre-emptive behavior at worst. First, adversaries of the United States begin to exploit vulnerabilities in American systems through asymmetric methods in space, cyberspace, and information domains. Second, it encourages countries like China and Russia to deploy capabilities to deny access to certain areas. Finally, American technological superiority is leading Russia and China to increase human intelligence operations on American territory and in allied countries, particularly in the area of espionage.

The superior technological capabilities of the United States for intelligence purposes, while offering clear advantages in anticipation, detection and targeting, also result in the increasing reliance of asymmetric techniques and operations by adversaries. It is now incumbent upon the United States to cooperate more with the allies to mitigate the vulnerabilities exploited by its adversaries.

## The Future of Five Eyes

The Five Eyes partnership, the most advanced institutionalization of intelligence sharing between the United States, United Kingdom, Canada, Australia and New Zealand, has its share of advantages and disadvantages for less powerful partners like Canada or Australia and is faced with many challenges in the era of multipolarity.

One of the most important challenges in the era of competition between the great powers is understanding new technologies and taking into account new areas of confrontation such as cyberspace. The Five Eyes and member countries at the national level have a role to play in ensuring intelligence efficiency in today's environment. For example, Australia has established a National Intelligence Scientific and Advisory Council, tasked with providing a more strategic and structural approach to technological change and its impact on the Australian intelligence community. This type of initiative could be developed within the Five Eyes to allow new opportunities for cooperation in the fields of technology and science. An integrated approach would allow member countries of the Five Eyes to benefit from each other's efforts. To go even further, each country could focus on one or more areas in which it can provide greater expertise and make this expertise available to its partners. This type of cooperation would save resources while filling the gaps in national intelligence apparatuses with the expertise that others have to offer.

The regionalization of threats, particularly in Southeast Asia, also raises the question of cooperation between the Five Eyes and other countries, such as Japan. Without necessarily going as far as the idea of a complete and institutional integration of other countries within the Five Eyes, it would however be appropriate to think of a form of expansion, according to geographic criteria or types or nature of threats, and to introduce, without necessarily integrating, other countries for deeper and lasting cooperation on a particular subject. Japan could, for example, be brought into the Five Eyes for deeper cooperation on the Chinese threat in Southeast Asia.

## The "Canadianization" of Intelligence

While multipolarity and great-power competition provide many opportunities for the Five Eyes, there remain some challenges in intelligence cooperation for countries like Canada. Indeed, while this brings many benefits to Canada - as a huge source of raw and finished foreign intelligence, Canada heavily relies on intelligence shared by its allies since it lacks a foreign intelligence service that collects, centralizes and covertly coordinates foreign human intelligence (HUMINT) outside its borders. This "producer bias" therefore reflects the interests and priorities of the recipient country and carries with it the considerable risk of being manipulated or of serving foreign interests rather than those of Canadians.

In the world of intelligence sharing, the ability to acquire intelligence represents a form of power where information is a bargaining chip. These mutual exchanges can therefore be used as a means of persuading partners to comply with a foreign nexus. This is especially true for Canada, given that it is far more often a consumer than an author of foreign intelligence products. This lack of input has earned it a reputation, among some of its partners, of being perceived as a "free-rider" to the detriment of a more active contributor role to intelligence sharing. This feeling is fuelled by two distinct realities. From the outset, its privileged position within the Five Eyes, but also the geographical circumstances of its territory which positions it directly within the defence and security perimeter of the United States.

It is therefore in Canada's interest to develop its capabilities in this area, either through a foreign intelligence service - which, however, seems unlikely at the moment for various reasons - or through a "Canadianization" of data collection and foreign intelligence analysis. By providing a larger Canadian contribution, Canada would position itself to be taken more seriously and to demonstrate that quality is sometimes better than quantity.

**By providing a larger Canadian contribution, Canada would position itself to be taken more seriously and to demonstrate that quality is sometimes better than quantity.**

Recommended by Stephanie Carvin and Thomas Juneau, this "Canadianization" is defined as a "constellation of initiatives aimed at orienting the collection and analysis of foreign intelligence towards a clearer and stronger pursuit of uniquely Canadian interests, as opposed to the receipt of raw and finite information which may or may not reflect a connection to Canada." Although nascent and scattered, this phenomenon is likely evolving within the national security and intelligence community. For the moment, this phenomenon is only the result of a series of small initiatives and not of a coherent and elaborate strategy, but it nevertheless constitutes an interesting, feasible and realistic alternative. In addition, strengthening the benefits of the latter would make it possible to produce independent assessments that are more tailored to Canadian needs which, in turn, should better support decision-making and thus lead to more efficient and coherent policy-making.

The "Canadianization" of foreign intelligence is not an approach that is mutually exclusive to other alternatives, but runs parallel to the common goal of enabling Canada to better respond to its interests and priorities. Similarly, it should not be seen as an alternative that aims to undermine the process of strengthening intelligence cooperation, but rather positions Canada as a better collaborator by contributing more, in a positive and active way, to its intelligence partnerships. This new posture would provide the opportunity for Canada to shape the narrative of transnational issues by offering a distinct perspective specific to Canadian values and priorities.

However, based on this observation, it would first be necessary for these Canadian values, priorities and needs to be better defined for such products to see the light of day and this is unfortunately not something that our political decision-makers seem to be interested in settling at present. Certainly, Canadian foreign intelligence capabilities are lacking at many levels, but a clearer definition of Canada's foreign policy priorities would support "Canadianization."

The next step would be to think about what could be done to encourage the continuation of this trend in Canada. It is clear that a better integration of the efforts of the NSI community is required in order to better face the emerging threats, because the evolution of the environment of the latter no longer allows neglect and mistakes in anticipating threats without having significant consequences for the security and prosperity of Canada.

## Considerations for Canada in Terms of Cooperation

It is with these risks in mind that the pursuit of "Canadianization" is strongly recommended for the NSI community to continue its collaborative efforts with the departments and agencies of the public service that are not traditionally involved in national security and intelligence matters. The same is true for new nongovernmental targets, whether they be universities, centers of excellence, think tanks, private companies, or the media. Indeed, the reality is that the intelligence services no longer have a monopoly on information and that the expertise and knowledge required to face threats require a more multidisciplinary approach. These resources and skills can be made available by the various non-governmental actors through closer collaboration.

Therefore, in order to better understand these new threats and the possible mitigation measures, it would be appropriate for the NSI community to invest more seriously in a continuous and horizontal

engagement with new non-governmental targets in order to build and maintain a mutual and consolidated trust. Full collaboration could make civil society and the Canadian private sector more aware of emerging threats. Additionally, although it has grown in recent years, it would help build intelligence literacy across all affected sectors, as the NSI community remains nebulous for many sectors and senior officials. Therefore, through awareness-raising and transparency actions, it should be better able to convey to external actors its role, priorities, limits, what it needs to be effective and how it can be used realistically. The clarification of its needs and its real capacities remains to be better defined and could possibly address and break down the silo mentality between the Canadian population and the NSI community.

An interesting line of thought for achieving this outcome is through an initiative similar to the collaborative research project *Public Intelligence* or the *Open Source Enterprise* established by the Director of US National Intelligence. Under the responsibility of the National Security and Intelligence Advisor in the Privy Council Office, this resource would act as a central database for exploiting open sources of all media - print, broadcast and online. It would also aim to bring together the collective contributions of independent researchers, universities, centers of excellence, think tanks, private companies and the media. It would also include reports and publications from various departments and agencies of the public service, such as the various strategic plans, annual review and oversight reports as well as assessments of current threats affecting different Canadian sectors. This framework would be accessible to all Canadian citizens in a public and transparent manner.

The benefits of such a project seem relevant and deserve special consideration since, it would make it possible to take advantage of the expertise of actors in the public and private sector in order to make Canada and Canadian citizens more resilient to threats. Indeed, in one way it would allow the NSI community to improve its methods and potential mitigation measures and on the other hand it could foster an electorate that further supports its important work and activities. Private companies, on the other hand, would get support in achieving their goals and objectives of innovation and prosperity. Civil society would benefit from a platform that would equip them to better advocate for and protect the security, rights and freedoms of Canadians. In short, from a mutual benefit and concerted action perspective, supporting the development of knowledge in the face of emerging and constantly evolving threats would only make external actors want to share more with those in the NSI community.

On the other hand, within the national security and intelligence community itself, better inter-agency cooperation and an information exchange process need to be emphasized. The divergent priorities, resources, and activities of the various stakeholders generate communication problems and misunderstandings which hinder an optimal response to requests for information, but also to decisions taken by the government. While it appears to have improved significantly, even greater coordination is needed within the community to address issues that hamper inter-agency cooperation. Indeed, bureaucratic competition, a distinct internal vocabulary, standard operating procedures, conflicting interpretations and different security clearances do not help provide an optimal response to the threats facing Canada.

Therefore, an approach similar to the *One Vision* framework, which aims to improve cooperation and simplify the process of information exchange between CSIS and the RCMP, should be scaled up and implemented across the NSI community. Of course, this would require an unprecedented level of national and international policy coordination, but it would help foster multidimensional inter-agency cohesion. As such, it would require the full integration of the efforts of different departments and ministries to address the challenges of different organizational cultures and procedures to provide a better response to the threats facing Canadian society.

## Conclusion

All in all, if the desire is really to better alleviate the problems associated with the emergence of new threats and to meet the many challenges arising from the current transition of power and the intensification of strategic competition between the great powers, it is necessary to call for innovation, as well as for an unprecedented fusion of knowledge, practices, planning and cultures from all affected sectors. At the same time, allies and states with similar democratic priorities and values must understand that their national interests are best served through intelligence cooperation and aligned action.

Moreover, if Canada is to fully benefit from multilateral intelligence cooperation, it must be able to do more by itself and for itself. The more Canada is able to actively contribute, the more it will get in return. This "Canadianization" of intelligence would add value to Canada as a partner and allow it to serve interests that reflect its priorities and values.

In conclusion, in order to make Canadian businesses and citizens more resilient in the face of threats, it is recommended that the NSI community establish a multilateral framework for cooperation and mutual assistance with various external actors. Through iterative and systemic engagements, community stakeholders must establish links with other sectors of Canadian society and draw on all of their specialized knowledge and skills to deal with the ever-increasing complexity of evolving threats.