UNCLASSIFIED

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Interview Summary: Global Affairs Canada (David Morrison, Alexandre Lévêque, Weldon Epp, Philippe Lafortune & Tara Denham)

Senior officials from Global Affairs Canada ("**GAC**") were interviewed in a panel format by Commission Counsel on June 15, 2024. The interview was held in a secure environment and included references to classified information. This is the public version of the classified interview summary that was entered into evidence in the course of hearings held *in camera* in July and August 2024. It discloses the evidence that, in the opinion of the Commissioner, would not be injurious to the critical interests of Canada or its allies, national defence or national security.

Notes to Readers:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Witnesses

[1] David Morrison is the Deputy Minister of Foreign Affairs ("**DM FA**"). He was appointed to this position in October 2022. Before this, Mr. Morrison served as the Foreign and Defence Policy Advisor to the Prime Minister ("**FDPA**") from 2018 to 2022 and as Deputy Minister for International Trade from January 2022 until October 2022.

[2] Alexandre Lévêque is the Assistant Deputy Minister for Europe, Middle East and Arctic.

[3] Weldon Epp is the Assistant Deputy Minister for the Indo-Pacific.

[4] Philippe Lafortune is the Director General, of the GAC Intelligence Bureau ("**IND**"). He has held this position since September 2022.

[5] Tara Denham is the Director General of the Office of Human Rights, Freedoms and Inclusion ("**IOD**"). She has held this position since September 2022. From May 2016 until August 2019, she was the Director of the Centre for International Digital Policy ("**IOL**"), which houses the G7 Rapid Response Mechanism ("**G7 RRM**"), including the RRM Secretariat and the RRM Canada team.

2. Toolkit against FI

2.1. Monitoring, Analysis and Reporting

2.1.1. RRM Canada

[6] Ms. Denham explained that the G7 RRM was created as a result of a Canadian initiative at the 2018 G7 Summit held in Charlevoix, Quebec. The G7 RRM was created to address threats to democracy. While the initial focus was on disinformation also referred to as foreign information manipulation and interference ("**FIMI**"), the mandate remains broader. Each G7 RRM member has identified a focal point, which is an individual that enables information sharing and engagement with the G7 RRM. The focal point may be based with a foreign ministry or a domestic department, depending on national areas of expertise or interests as it pertains to foreign threats to democracy. Canada leads the RRM Secretariat on an ongoing basis, which enables information sharing, produces annual reports, coordinates working groups, and will support any potential coordinated responses.

[7] RRM Canada is the technical team located at GAC. This team has the capability to monitor the online environment for indicators of potential FIMI. As of 2024, there are eight technical analysts.

[8] The GAC representative to the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") during election cycles is the Director of the IOL. The GAC representative participates as a representative of the department as well as lead for the G7 RRM team. During the General Elections ("**GE**") in 2019 and 2021, RRM Canada supported SITE TF by providing open source research and analytics on indicators of

potential foreign interference in the online environment in Canada, along with any information shared via the G7 RRM on evolving threat tactics.

[9] In 2023, the Prime Minister directed the activation of the SITE TF to monitor by-elections. The GAC representative, along with the RRM Canada team, was required to devote a large portion of their limited resources to monitoring the Canadian information environment. These resources would otherwise have been directed to monitor the international environment to identify and report on evolving FIMI tactics by known threat actors aligned with RRM's international mandate (e.g., producing assessments of Russian FIMI campaigns and tactics in the context of the war in Ukraine, Chinese FIMI tactics, etc.). In an email she wrote in May 2023, Ms. Denham identified to Government of Canada counterparts the need to review the membership of SITE, noting the mandate of RRM Canada is international in nature. Should capabilities that the RRM has be required to monitor the domestic information environment, consideration should be given to establishing such functions within a domestic department.[1] Mr. Morrison echoed this concern, stating that it was not sustainable for RRM Canada, a division of GAC, to be responsible for monitoring the domestic information environment for disinformation on an ongoing basis. He noted that Budgets 2022 and 2023 provided funding to combat FI to Public Safety ("**PS**"), Elections Canada ("**EC**") and Privy Council Office ("**PCO**") – Democratic Institutions. This funding could enable the appropriate domestic organization to develop a monitoring capability aligned with their mandate. Mr. Morrison noted that conversations are ongoing about building capacity for domestic monitoring within domestic departments. He expressed his hope that RRM Canada would not have to devote the same level of resources to SITE TF operations in the next election as it did in past elections, because sufficient capacity would have been developed within domestic departments.

[10] Ms. Denham said that RRM Canada has had some engagement with Tencent [WeChat's parent company]. She explained that RRM Canada typically engages with social media platforms once it notices indicators of foreign information manipulation,

[1] CAN031488.

and shares the information with social media platforms to inform their own decisions as to whether activities violate their terms and require action. Mr. Morrison believed that this type of engagement could potentially prove fruitful. He explained that engagement with social media platforms associated with hostile states such as the People's Republic of China ("**PRC**") was not impossible, as they have a presence in Western countries and ultimately wish to remain legitimate and profitable.

2.1.2. Information-sharing

[11] Mr. Morrison explained that GAC is both a producer and consumer of intelligence.[2]

[12] GAC produces intelligence in two ways. First, it produces diplomatic reporting, some of which is classified, including reporting on security issues through the Global Security Reporting Program. Second, GAC assesses the intelligence it receives from the Security and Intelligence ("**S&I**") community, adding insights from its unique foreign affairs perspective, and produces intelligence assessments. GAC's intelligence is shared within the Government using Slingshot, and with like-minded foreign partners through GAC's Intelligence Liaison Officer Program.

[13] GAC is also a consumer of intelligence. Mr. Lafortune explained that as the DG Intelligence, his team receives intelligence from the S&I community on behalf of GAC. He is also responsible for internal distribution of the intelligence. When the distribution list for a specific intelligence product is limited and he feels that the product could be useful for a specific already cleared individual within GAC who was not granted authorization to see it, he may ask the producer of the intelligence for authorization to share the document more broadly, and these requests are usually granted.

2.1.3. CSIS TRM approvals

[14] Mr. Lafortune explained GAC's role in approving high risk CSIS Threat Reduction Measures ("**TRMs**"). Bill C-51 established a new TRM mandate for CSIS in 2015. Under the four-pillar risk assessment required by policy for TRMs, GAC provides a foreign policy risk assessment for each TRM with a foreign nexus. If any pillar of the TRM is

[2] CAN028130.

assessed to be high risk, on top of their own chain of command/governance, CSIS must obtain approval from the Deputy Minister ("**USS**") or Minister ("**MINA**") of Foreign Affairs before proceeding.[3]

[15] In 2023, CSIS and PS drafted a Governance Protocol on Threats to Parliamentarians. The Protocol was created to operationalize the Minister of Public Safety's *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*. Briefings mandated by this Ministerial Direction can be done pursuant to CSIS's authority to conduct TRMs. TRMs with a foreign nexus, require a foreign policy risk assessment from GAC. Given the requirements under the 2023 Public Safety Ministerial Direction, TRMs requiring approval from USS or MINA would have to be approved several times due to parallel governance mechanisms. GAC noted that this would be duplicative since, under the Protocol, GAC already provides input through inter-departmental committees. As a result, the requirement in the Protocol for USS or MINA to approve high risk TRMs was removed by Public Safety, with the consent of GAC.

2.2. Public Attribution (*Naming and Shaming*)

[16] Ms. Denham discussed the intricacies of GAC's cyber attribution framework. The framework's purpose is to outline the process for the Government of Canada ("**GoC**") to decide whether to publicly attribute to the responsible state a malicious cyber-attack directed at the cyber networks of Canada or its allies. The framework complies with related international conventions.

[17] Mr. Morrison explained that GAC does not have a similar attribution framework for FIMI. This is for two reasons. First, unlike for cyber-attacks, there is no international convention on FIMI. Second, it is easier to determine and attribute responsibility for a FIMI campaign, since the motivations for such campaigns are more obvious than for

[3] Any TRM for which one of the four risk pillars (foreign policy, operational, reputational or legal) would be assessed as high.

cyber-attacks. That said, there are other processes for going public about FIMI, or for other FI activities.

2.3. Engagement with Diasporas

[18] Mr. Morrison said that GAC's engagement with diaspora communities in Canada is limited, and that any engagements that take place are to inform and advance Canada's foreign policy objectives. In this context, GAC does meet with organizations within Canada, which may include members of diaspora groups, to discuss human rights issues. This can be beneficial to GAC, particularly when meeting with groups or individuals that can share information related to a country. As an example, he referred to a May 31, 2023, GAC workshop with the Canadian Coalition on Human Rights in China.[4] [A list of such consultations can be found in the GAC Stage 2 Institutional Report.]

2.4. Diplomatic Responses

[19] Mr. Morrison agreed that a document that Commission Counsel referred to provides a good synthesis of the different GAC tools for countering FI.[5] However, simply listing these tools misses an important aspect of GAC's work to counter FI – maintaining a live, ongoing discussion with foreign states, even adversarial ones. This, according to Mr. Morrison, is the essence of diplomacy: how you work a relationship with a government that may be adversarial, dealing with a diversity of topics and managing the to-and-fro / cut-and-thrust of the relationship. Some of this is done formally, some of it informally. Mr. Morrison underlined that well-known public measures such as declaring a diplomat *persona non grata* ("**PNG**") or imposing sanctions may be legitimate tools to counter FI, but there is a significant cost to using them, as doing so may jeopardize Canada's ability to advance our national interests, including by maintaining discussions and relationships

[4] CAN024044.
[5] CAN025180.

with certain states. That said, PNG and sanctions are always on the table, and have been used as deemed appropriate, on multiple occasions in recent years.

[20] Mr. Epp noted that GAC's work in countering FI is only partially visible to the general public, possibly because most of GAC's work is done through diplomatic channels. He noted that the effectiveness of the diplomatic toolkit must be understood in the context of the related actions of domestic partners, such as disruptive activities like threat reduction measures (TRMs.). He explained that GAC has to consider a number of different and sometimes competing interests when deciding the appropriate diplomatic response to events: for example, consular cases, economic interests, public confidence, and international credibility. Thus, the diplomatic response is tailored to the objectives for each case, ranging from quiet diplomacy to the extreme of severing diplomatic relations entirely.

[21] Mr. Epp also stated that diplomatic efforts will often start quietly and then increase as needed. The repeated raising of an issue in each meeting and raising it at increasing levels can be effective in communicating a warning, while the subsequent denial of visas to incoming diplomats from that state communicates a consequence. The selection of diplomatic tools may also be intended to communicate with other countries or the public, rather than just the offending state. PNGing tends to be public, and therefore also communicates to other would-be adversarial states that consequences are real. He noted that GAC had been systematically putting the PRC on notice that FI activity is a core issue for Canada, and failure to address it would have consequences.

2.4.1. Writ Period Protocol Circular Notes

[22] Mr. Morrison agreed that writ period protocol circular notices are a means to counter FI, but are more of a reminder of what activities are within and outside of the Vienna Convention given foreign states are already aware that they are not allowed to interfere with democratic processes in Canada. This is a long-standing rule that all states know. GAC has also specifically briefed PRC diplomats on Canada's expectations.

2.4.2. Démarches

[23] Mr. Morrison explained that a “démarche” is a formal state-to-state communication through diplomatic channels that can convey information, a request, or a clear Canadian position on an issue.

[24] Mr. Morrison explained that there is a hierarchy for démarches in the world of diplomacy. A call from a mid-level official to a foreign mission carries less weight than a call from the Minister. A phone call may be less significant than a diplomatic note or a face-to-face meeting.

[25] Mr. Morrison was asked about a classified document. He distinguished diplomatic démarches from the engagement of CSIS with its counterpart intelligence agencies. CSIS uses its formal relationships with its international counterparts to advance certain issues very effectively. When these formal channels are used to convey messages that impact international relations, CSIS consults and coordinates with GAC. Otherwise, GAC would not be consulted about such actions by CSIS unless CSIS intended to conduct a TRM, which would require it to obtain a foreign policy risk assessment.

2.4.3. Sanctions

[26] Mr. Morrison stated that sanctions are rarely used as a counter-FI tool but are fairly common in other circumstances. He noted that Canada did use sanctions in response to Russian actors conducting disinformation campaigns targeting Ukraine.

3. Specific Issues

3.1. Declaration of Zhao Wei as PNG

[27] Mr. Morrison explained the sequence of events that led to Zhao Wei, a PRC diplomat, being declared PNG. Well before the issues of PRC Overseas Police Stations and the eventual PNGing of Mr. Zhao, GAC had conducted numerous démarches, at increasing levels, to warn against further FI, and had begun to convey that this behavior had consequences for the PRC. In this continuum of increasing pressure and consequences, PNG and other public tools were never off the table.

[28] In 2021, CSIS shared intelligence with GAC on more than one occasion regarding the PRC's interest in MP Michael Chong. In March 2021, China imposed economic sanctions on Mr. Chong, as well as other MPs.

[29] On May 1, 2023, the Globe & Mail reported that Mr. Zhao had participated in PRC's efforts to "target" Mr. Chong. This introduced additional considerations: options to make the PRC "pay a price" for FI now came with more pros and less cons.

[30] On May 2, 2023, CSIS shared intelligence – which did not relate to Mr. Chong – with GAC that had been shared previously in 2021, but at that time had not moved beyond the working level at GAC. For GAC, this intelligence completed the picture regarding earlier suspicions concerning the legitimacy of Mr. Zhao's behavior in Canada.

[31] Mr. Epp noted that while Canada is not required to provide a reason for declaring any particular diplomat PNG, it may be helpful to leverage specific intelligence as a cause.

[32] On May 4, Mr. Morrison called in the PRC Ambassador in Canada to advise that Zhao's position in Canada was not tenable. GAC's proposed approach would require the PRC to own the issue. The approach could also limit the risk of retaliation. In the end, the decision was taken to declare Mr. Zhao PNG.

[33] Mr. Morrison noted that by this point, Canada had warned the PRC about its FI activities 30 times at all levels since January 2022, including Prime Minister Trudeau raising the issue with President Xi.

[34] On May 8, the Associate Deputy Minister Cindy Termorshuizen demarched the PRC Ambassador and advised him that Mr. Zhao was officially PNG and must leave Canada. The PRC retaliated by declaring Canada's Consul in Shanghai PNG. Mr. Morrison noted that a response of this type was to be expected, and did not come as a surprise.

3.2. Murder of Hardeep Nijjar

[35] Mr. Morrison discussed GAC's response to the June 18, 2023, murder of Hardeep Nijjar, and the strain this issue brought to Canada's bilateral relationship with India.

[36] Mr. Morrison explained that the events occurred against the backdrop of India's long-standing complaints regarding what it considers to be Canada's soft approach to Khalistani extremism.

[37] Between June and August, 2023, CSIS prepared various assessments in relation to this matter. Relevant intelligence and assessments were briefed to various senior officials including those at GAC.

[38] On August 17, 2023, the NSIA at the time (Jody Thomas) travelled to India as part of a pre-planned visit to prepare for the upcoming G20 summit. She used the opportunity to inform Indian officials that the GoC had indications of Government of India (GoI) involvement in Mr. Nijjar's murder.

[39] On August 23, Mr. Morrison contacted his counterpart in the Indian government, Secretary (East) Saurabh Kumar, to inform him that Canada had serious concerns related to the murder of Mr. Nijjar.

[40] On August 27, 2023, Minister of Foreign Affairs Mélanie Joly had a call with her Indian counterpart. She conveyed Canada's serious concerns about the indications of GoI involvement in the murder.

[41] In September, NSIA Jody Thomas, CSIS Director David Vigneault, and Mr. Morrison, in his role as Deputy Minister, met with counterparts in New Delhi to continue pressing Canada's concerns. On September 11, PM Trudeau did the same with Indian PM Modi on the margins of the G20 Summit Delhi. In all instances, Canadian officials conveyed to their counterparts that the information about GoI involvement was likely going to become public soon, given (1) the risk of media leaks, (2) the United States unsealing an indictment in a related case, or (3) the RCMP investigation. PM Modi and his officials rejected the accusations and denied any GoI involvement.

[42] On September 18, 2023, the Globe and Mail published an article stating that Canadian intelligence officials had information about potential Indian government involvement in the murder of Mr. Nijjar. Following the publication of the story, Mr. Trudeau publicly announced in the House of Commons that Canadian security agencies had been

actively pursuing credible allegations of a potential link between the agents of the government of India and the killing of Mr. Nijjar.

[43] Canada declared an Indian diplomat PNG. In response, India declared a Canadian official PNG, demanded "parity" in diplomatic presence, effectively expelling 41 Canadian diplomats from India, sponsored a FIMI campaign against Canada[6], and suspended visa services to all Canadians on September 20, 2023. Canada's diplomatic actions included further bilateral diplomacy, coordination with partners around the world to amplify diplomatic messages, and suspension of trade talks and a planned Team Canada trade mission, among other steps.

3.3. PRC Overseas Police Stations ("OPS")

[44] Mr. Epp explained that GAC learned of the existence of PRC OPS on Canadian soil through the September 2022 report published by a non-governmental organization called Safeguard Defenders. The NGO's report stated that PRC OPS were used to implement PRC operations to harass, intimidate and punish individuals around the globe with the aim of returning "fugitives" to the PRC. Ms. Denham explained that RRM Canada played an important role in confirming the accuracy of the Safeguard Defenders report.

[45] Mr. Epp explained that PRC OPS were hybrid in nature. They offered useful services to Chinese citizens in Canada (e.g., renewing ID cards). But they were in a 'grey zone' and also offered a potential platform for transnational repression. Indeed, some of the reported PRC OPS activities globally constituted FI transnational repression. Regardless of whether this was the case in Canada, the stations were clearly illegal as a matter of jurisdiction, functioning like a foreign mission but without GoC authorization and therefore acting outside of the rules of the *Vienna Convention*.

[46] Mr. Morrison said that the COVID pandemic likely explained in part the growth of PRC OPS. For example, Chinese nationals cannot normally get divorced outside China, but

[6] CAN025923.

because of travel restrictions during the pandemic, PRC OPS were granted the right to authorize divorces. This led to an increase in demand for their services.

[47] Mr. Epp described the steps that GAC undertook to respond to the PRC OPS.[7]

[48] On October 7, 2022, GAC made representations to the PRC Ambassador to Canada, requesting detailed information about the OPS and asking the PRC to end any activities not permitted by the *Vienna Convention*.

[49] On October 28, 2022, GAC made further representations to the PRC Ambassador, which included presenting a diplomatic note insisting that the stations be shut down. Throughout this period GAC coordinated closely with diplomatic partners also affected by PRC OPS.

[50] On February 24, 2023, GAC presented another diplomatic note to the PRC Ambassador.

[51] Parallel to these GAC initiatives, the RCMP investigated the PRC OPS. On June 13, 2023, the RCMP informed the House of Commons Standing Committee on Procedure and House Affairs that any PRC "policing activity" that was being done had been shut down and that investigations were ongoing.[8] During 2023, Canada initiated efforts leading to greater commentary on FI in statements of the G7.

3.4. WeChat Disinformation campaign targeting MP Michael Chong

[52] Ms. Denham discussed the June 28, 2023, RRM Canada Open Data Analysis Report, "WeChat Account Activity Targeting Canadian Parliamentarian Suggests Likely State Involvement." She explained that in summer of 2023, RRM Canada was monitoring Canada's information environment as part of SITE TF's work during the 2023 by-elections. During this period, RRM Canada detected a potential FIMI operation on WeChat between May 4 and May 13, 2023, which was unrelated to the by-elections but was targeting MP Michael Chong.

[7] CAN023929.

[8] CAN023929.

[53] A number of factors led RRM Canada to have a high level of confidence that the FIMI campaign was linked to the PRC:

- One-third of the accounts were known state media outlets and accounts that are likely linked to the PRC;
- Two-thirds of the accounts were anonymous accounts for which links to the PRC were opaque, and which had not previously published any news stories on Canadian politics;
- The campaign was coordinated in timing and coincided with Canada's declaration of Mr. Zhao as PNG.

[54] Mr. Morrison stated that the FIMI campaign targeting MP Chong on WeChat was much different than the disinformation that was reported by Kenny Chiu during GE44. In Mr. Chiu's case, the disinformation had originated from four Canadian websites with no known links to the PRC; while in Mr. Chong's case, the RRM Canada team was able to identify 72 accounts amplifying the information that had known links to the PRC.

[55] Ms. Denham stated that GAC issued a public statement informing Canadians of the FIMI campaign targeting Mr. Chong. The statement was translated into Mandarin to maximize its reach to Chinese-speaking communities in Canada.

3.4. Spamouflage campaign

[56] Ms. Denham explained that on September 5, 2023, RRM Canada received a notice from counterparts that a bot network connected to the PRC was targeting dozens of Canadian parliamentarians on Twitter, Facebook and YouTube.[9] Targets included the Prime Minister, the Leader of the Opposition, several members of Cabinet and backbencher MPs across the political spectrum and from multiple regions of Canada.

[57] Beginning in early August 2023 and accelerating in scale through the beginning of September, the bot network left thousands of comments on various online platforms in

[9] CAN025903.

English and French. The campaign altered online content, originally created by Mr. Xin Liu, a critic of the PRC residing in Canada, to make it appear as though he was accusing various MPs of criminal and ethical violations. Mr. Liu never created or posted the content. RRM Canada and CSE believed it likely that these videos were “deep fakes” [AI-generated impersonation videos].

[58] Ms. Denham noted that this constituted the first time that RRM Canada became aware of a specific spamouflage campaign employing “deep fakes.” [“Spamouflage” is a network of new or hijacked social media accounts that posts and amplifies propaganda messages across multiple social media platforms. The word is a portmanteau of “spam” and “camouflage,” intended to portray the covert and hidden attempts to spread spam-like content and propaganda among more benign, human-interest style content].

[59] Mr. Morrison said that the quality of the spamouflage campaign was mediocre; it had been poorly executed, could easily be identified as AI-generated and produced little to no engagement. However, Mr. Morrison recognized that this is the early stages of China engaging in this type of FIMI campaign. He said that this would become an increasingly important threat as technology improved in future.

4. Policy Discussion

[60] Mr. Morrison was asked whether it would be advisable to encourage the international community to develop an internationally-recognized definition of FI. Mr. Morrison replied that this would not be feasible given the geopolitical situation; such a consensus could never be reached. In his view, however, it is not necessary; the rules of diplomacy are well known, if countries choose to follow them. He is confident that Canada’s diplomatic activity, while aggressive at times, does not cross any lines and could not be construed as FI, as it is done in an overt fashion.

[61] Mr. Lafortune noted that Bill C-70 amends section 16 of the *CSIS Act*. This should enhance the ability of CSIS to collect foreign intelligence on behalf of GAC, addressing a specific technical gap resulting from a 2018 Federal Court decision interpreting section 16.