PROTECTED B

Deputy Ministers' National Security Committee Meeting: Retreat
July 7, 2021
PCO Secure Mobile
Time: 09:30 – 11:30

Overview: This is an extended (2 hour) Retreat dedicated to an open discussion on the national security governance structure and potential improvements. The Agenda and Secure Mobile Conference Call Instructions, can be found in **TAB A** (instructions yet to be provided). The next meeting is scheduled for mid-August 2021.

STANDING ITEM #1 – OPENING REMARKS – 5 MIN
PS and DND will provide opening remarks. A meeting summary of the June 1, 2021 meeting is in **TAB B**.

ITEM #2 – OPEN DISCUSSION ON NATIONAL SECURITY GOVERNANCE (PS/ALL) – 1 HR 50 MIN
PS has prepared a deck intended to provoke the discussion, rather than present a proposed position/options. Therefore, partners were not consulted on its development.

Background: This Retreat will focus on the national security (NS) governance structure, specifically pertaining to economic security (ES), cyber, and hostile activities by state actors (HASA). This will be an open-ended discussion to seek views from Deputies on what is needed for the future of Canadian NS governance. The objective is not to arrive at a solution, but instead provide the opportunity to share perspectives and insights as a first stage for longer-term policy development, and exploration of options that may range from incremental to sweeping changes. The proposal included at the end of the deck is intended to elate a discussion, not an interdepartmentally-supported way forward.

In terms of gaps and challenges, the deck notes that coordination is currently being undertaken from multiple fronts, and is more focused on feeding decisions up to Cabinet rather than providing strategic direction to departments and their operations. In addition, committee discussions at DMNS and other DM-level fora remain at the strategic level and do not effectively blend policy and operations, are reactionary to media or current events, and lack sufficient and sustained engagement with provincial, territorial, municipal, and private sector stakeholders. There is room for improvement in NS governance in order to meet the DMNS co-chairs' stated objectives of threat identification, risk management processes and decision-making, as well as stakeholder management, and responding to threats effectively and quickly.

RCMP Considerations: While the Retreat will centre on NS governance gaps and opportunities more broadly, the primary focus will be on ES, HASA, and cyber, given their particular interdisciplinary nature and upcoming policy proposals that would pose strong candidates as Cabinet vehicles to bring changes to the current governance frameworks. ES and HASA are two key areas of the Federal Policing's NS policy work, and cyber is of significance to both the Federal Policing National Security (FPNS) and FP Criminal Operations (FPCO) programs. The RCMP agrees with many of the gaps identified in the presentation, particularly that efforts to address these issues should be more than simply the sum of separate operational policies or disparate legislative tools that are currently employed. However, the absence of counterterrorism is notable, given that there continues to be challenges around interdepartmental coordination and operations in this realm.

[APG]

PROTECTED B

Given the interdisciplinary nature of the ES, HASA, and cyber threat environments, it is especially crucial to have strong interdepartmental information sharing processes in place as criminal or concerning activities are often subtle, covert, and multi-faceted. A standalone "fusion centre" similar to the Integrated Terrorism Assessment Centre (ITAC) hosted at the Canadian Security Intelligence Service (CSIS), or a "fusion cell" similar to the interdepartmental Security and Intelligence Threats to Elections (SITE) Task Force led by CSE, may be beneficial. The different communities involved in these threat areas (e.g. science-based and/or economic-based departments) will be implicated in different ways, and any solution will need to address or reflect the needs of all implicated decision-makers, at the appropriate level. It will also be important to educate partners on the criminal context in the ES, HASA, and cyber threat environments; for example, foreign states may use criminal networks to create more distance between their involvement in certain threat activities. This has been especially evident in the context of foreign direct investment under the *Investment Canada Act* but also applies in other circumstances including cyber threats.

The RCMP has significant equity in these discussions on NS governance, and will likely play a large role in potential future efforts to address policy and operational coordination issues across the NS community. While the enforcement role is not directly addressed in the deck, it remains a fundamental part of the GoC's response to this threat environment – whether through the laying of criminal charges, or through other means, including intelligence collection, disruption, deterrence, and prevention. Accordingly, the RCMP will need further investments in its Federal Policing program to better respond to the evolving threat landscape, including to help the GoC establish connections between states of concern and organized crime networks, cyber threat actors, and money laundering networks.

It cannot be overlooked that this upcoming discussion on NS governance is happening in tandem with other ongoing efforts to address foundational elements of the GoC's NS framework; namely, seeking funding to reset and renew the Federal Policing Program, including FPNS operations and supporting specialized services, and modernizing CSIS's authorities, and building institutional resiliency in the form of culture, recruitment and retention, transparency, accountability, information management, and technology solutions. In addition, the Centre on International Governance and Innovation (CIGI), a non-governmental think-tank, is working closely with senior GoC officials and other stakeholders to develop what it is purporting to be a reimagined NS strategy for the 21st century, expected to be published in Fall 2021. Finally, the statutory reviews of the *National Security and Intelligence Committee of Parliamentarians (NSICOP) Act* in 2022, and the five-year review of the *National Security Act, 2017* in 2024, will provide the community with the opportunity to assess whether these respective pieces of legislation have been able to meet their intended purposes, and to clarify any areas of uncertainty in the legislation. It is expected that most, if not all, noted initiatives will seek out international comparators, especially Australia and the United Kingdom, which have both undertaken NS modernization initiatives.

Economic Security (ES)

ES presents long-term, strategic threats that can be difficult to quantify, as the results may not manifest as a loss of a tangible asset or value; instead, it may represent a loss of potential or competitive advantage, and may not be felt for years. Threat actors may use proxies such as academic institutions, trade organizations or individuals, willing or coerced, to conduct these activities. Those impacted by ES threats go well-beyond the traditional NS community, presenting a challenge for effective governance, and are sometimes a point of divergent views between competing economic and security interests. While ES threats may reach the NS threshold for criminal investigations, other tools are more commonly used, in the administrative context (e.g. *Investment Canada Act*), *Criminal Code* provisions (e.g., frauds) or other legislation (e.g. theft of intellectual property).

[APG]

PROTECTED B

Hostile Activities by State Actors

HASA covers a wide range of harmful and complex threats posed by foreign governments and their proxies (persons, entities, and/or criminal organizations acting on their behalf). HASA can be conducted in different ways, but ultimately results in harm to Canada's national interest, such as our political system or democratic institutions and our social cohesion. Ongoing efforts to undertake HASA-related policy and program development are underway in several departments and agencies, including the RCMP. However, these efforts are not consistently reflected in broader community discussions.

Cyber

The pace of change has accelerated across the NS threat landscape given the exponential rate of evolution in cyber capabilities. Advancements such as encryption or double Virtual Private Networks have enhanced the abilities of threat actors, as well as organized crime groups, to communicate and conduct their illicit activities with relative impunity. These activities can include ransomware threats, network intrusions and data theft, online fraud scams, and money laundering, and often target Canadians' privacy, financial security, businesses, safety, and government institutions. Government decision-making and operational responses struggle to keep up with the velocity of these advancements, in particular given the reticence of victims to come forward to law enforcement given the financial or social impact that a cyber breach may have on their stakeholders' levels of trust (e.g. private companies, research institutions, municipal or provincial governments).

NS Authorities and Modernization

The deck notes some legislative authorities that contribute to the NS 'toolkit' for responding to threats, though a notable absence is the *CSIS Act*. At the June 1, 2021 DMNS meeting, CSIS provided an overview of their efforts to update authorities in line with the modern-day threat environment [redacted] Enacted in 1985, numerous shortcomings are impeding CSIS' ability to keep pace with certain threats, or requiring CSIS to rely on other partners to meet their objectives. Any changes to CSIS' governing legislation will have impacts on the broader NS community. The RCMP Federal Policing Program is the enforcing authority for NS investigations and works closely with CSIS through the One Vision program and other interagency coordination to address and respond to NS threats to Canada. Accordingly, discussions around NS governance should take heed of this developing context.

Institutional Resiliency: culture, recruitment and retention, transparency, accountability, IM/IT

With regards to the wider context in which this governance discussion is taking place, Deputies recognized at the DMNS meetings on April 8, 2021, and June 1, 2021, that institutional resilience is needed across the NS community, and requires a cohesive approach. While these challenges are faced across the GoC, the unique nature of the work done by the community requires tailored solutions.

With respect to culture, recruitment, and retention, efforts have been undertaken in recent years to rectify these gaps. However, overall progress has been slow, and Canadians continue to perceive the NS community as being homogenous and unrepresentative of the Canadian population.

[APG]

PROTECTED B

Regarding accountability, departments and agencies are grappling with pressures relating to external reviews of their national security mandates. As the number of reviews and requirements increase, pre-existing resource constraints, inadequate IT infrastructure and competing operational priorities are impacting the capacity to adequately respond to requests, address findings, and implement recommendations. In addition, the various initiatives of the NS Transparency Commitment should be aligned to ensure that efforts are coordinated and have stronger impact. Finally, information management and technology solutions are important elements of the RCMP's ability to conduct its operations, exchange information with partners, and comply with document production as required under Access to Information frameworks and external reviews. There are inefficiencies and redundancies brought through the incompatibilities of different systems, including secure communication networks and encryption across departments.

When discussing NS governance, the above-mentioned elements that aim to build institutional resiliency must inform any forward-looking plans for the NS community. A redesigned NS governance structure must not only provide leadership on NS policy and operations, but also assess progress in these key areas which enable that very work to take place. In addition, any changes to NS governance could incorporate relevant recommendations from external review bodies and the NS-Transparency Advisory Group, and be reflected in the anticipated public-facing NS Strategic Overview.

NSICOP Act (Bill C-22) and the *National Security Act, 2017* (Bill C-59)

The statutory reviews of the *NSICOP Act* and the *National Security Act, 2017* will take place in 2022 and 2024, respectively. These reviews provide an opportunity to assess whether the RCMP is positioned to keep pace with the changes brought about by the legislation (e.g., an increase in the volume of external reviews that the RCMP is subject to). More broadly speaking, these reviews will also assess whether the legislation met their intended purposes. With respect to the *NSICOP Act*, the intended purpose was to take a non-partisan approach to national security and intelligence issues in Canada, by creating an all-party committee to monitor and review departments and agencies with national security responsibilities. The intentions of the *National Security Act* were predicated upon accountability, threat reduction, and data analytics. It established both the National Security and Intelligence Review Agency, as well as the and the Office of the Intelligence Commissioner; it also updated some CSIS authorities including a justification framework for CSIS or those acting at its direction to engage in activities that would otherwise constitute offences. Any wide-reaching changes to NS governance, beyond ES, HASA, and Cyber, may be well placed in such a legislative review.

CIGI: A Reimagined National Security Strategy for the 21st Century

CIGI, a non-governmental think-tank, set out in Fall 2020 to draft a new national security strategy for Canada. This work is being informed by GoC senior officials (ADM-level) as well as the private sector, academia, and civil society. The stated goal is to eliminate siloed assessments and policy frameworks and develop a holistic approach to dealing with modern national security risks. While the extent to which these recommendations will be adopted into future GoC NS-related governance decisions is unclear, it is worth informing this ongoing discussion with that project's findings.

[APG]

PROTECTED B

Talking Points:

Overall

- Thanks to PS for preparing this thought-provoking presentation. This is a welcome discussion and I support a comprehensive exploration of options that should range from incremental to sweeping changes of our NS governance.

- I agree with the identified gaps, and the need to address them collectively, as the potential solutions should absolutely be more than simply the sum of separate policies or legislative tools currently employed.

- Threat actors are learning our laws and regimes, including how to navigate or work around them. We need to remain vigilant, aware not only of current threats but emerging ones as well, with an eye to affecting all avenues - enforcement, disruption, deterrence, and prevention – to stop them.

- Given the interdisciplinary nature of the ES, HASA, and cyber threat environments, it is especially crucial to have strong interdepartmental information sharing processes in place, as threat actors are often targeting and testing different vectors in our laws and regimes.

- We know that foreign states of concern are using organized crime networks, cyber threat actors, and money laundering networks to further their goals. In our efforts to address these threats, we must not forget the criminal context of national security, and how national security investigations overlap with criminal investigations.

- From an RCMP perspective, a Canadian National Security Strategy is overdue. It needs to set clear objectives around what the Government wants to achieve and establish an action plan – it must be forward leaning and we must not be afraid to think big.

- Our ability to provide greater strategic direction could flow from it.

- A new NS governance structure could align to this Strategy. Seeing the current structure on one slide shows its inefficiency and significant overlap.

- With or without a NS Strategy, we should focus on streamlining the existing committees and bringing about greater cohesiveness to our collective objectives. We may also wish to rethink the membership of them, and keep in mind that the focus should be on providing more direction and horizontal management of the NS mandate across our organizations.

- [redacted] it is important to note that counterterrorism still remains a significant part of the NS threat environment. Any changes to NS governance should not be tailored too closely to ES and HASA needs, to the detriment of a governance framework that can also be responsive to counterterrorism and other yet-to-emerge threats.

[APG]

PROTECTED B

- We also need to determine what we want the scope of NS to be, within the Government of Canada. Are NS concerns being meaningfully addressed when woven through existing legislation and processes? This is especially important in the context of the *Investment Canada Act* or the *Telecommunications Act* and potential weaknesses in that decision-making structure.

- When it comes to working with our counterparts, especially in the Five Eyes, I do reflect on whether we are being seen as a 'weak link'. If so, what action would change that perception.

NS Authorities and Modernization

- A notable absence in the Key NS Tools on slide 5 is the *CSIS Act*, which among other key elements, defines threats to the security of Canada.

- The Service's current efforts to modernize the legislation will have impacts for the broader NS community, especially as it relates to enforcement. A new or revised NS governance framework should be informed by these anticipated changes.

- We support these efforts to modernize the *CSIS Act*. Along a similar vein, the RCMP needs to be better equipped to investigate, disrupt, prevent, and/or enforce the national security threats of today and tomorrow. As we develop our proposal, we will seek the community's support on increasing capacity for national security-related law enforcement, commensurate with the emerging challenges and pressures.

Building Institutional Resiliency

- As we discuss a new or revised NS governance framework, I also want to ensure we are inserting considerations relating to the institutional resiliency discussions held earlier this Spring.

- Namely, the culture, recruitment and retention, transparency, accountability, and IM/IT challenges we all face will continue. We need to ensure that the NS governance framework is not only providing leadership on NS policy and operations, but also assessing progress in these key areas which enable that very work to take place.

- A revised NS governance framework could also provide direction to departments on incorporating relevant recommendations from external review bodies and the Transparency Advisory Group, or even the Centre for International Governance and Innovation (CIGI) project, among others.

STANDING ITEM #3 – CLOSING REMARKS (PS/DND) – 5 MIN

PS and DND will lead this agenda item. The National Security and Intelligence Advisor may flag considerations relating to the potential need to develop Medium-Term Planning (MTP) proposals relating to national security, in anticipation of a potential federal election in Fall 2021. There are no RCMP issues that need to be raised at this time.

[APG]