Summary Report

Author: Alex Wilner, Associate Professor, Norman Paterson School of International Affairs, Carleton University, Ottawa, alex.wilner@carleton.ca

Panel Theme: Enforcing, Deterring and Prosecuting Foreign Interference Activities

Key Issues: Three themes animate this particular panel: enforcement, prosecution, and deterrence. I will focus my attention on the last of these three processes – deterring foreign interference in Canada. My contribution will focus on outlining how the core attributes of deterrence theory can be expanded and refined to deter foreign interference. My comments are based on a body of scholarly research I have advanced over the past two decades on applying deterrence to novel and emerging security considerations (e.g., deterring terrorism; deterring information warfare; cyber deterrence; AI deterrence)[1], and are derived from a recent journal article on the subject of deterring FI that I published with Dr. Marshall Palmer.[2] I argue that deterrence theory should be thought of and constructed as the core strategic purpose undergirding all counter-FI activities in Canada.

Assessment: To understand whether and how foreign interference might be deterred, it is necessary to first define deterrence and outline its key theoretical prerequisites and pathways.

At its conceptual core, deterrence is fundamentally about using a combination of threats to shape an adversary's behaviour in a way that meets our own objectives. It entails convincing another actor – who remains able to behave in ways that are detrimental to us – to willingly forgo an action we would rather they not pursue. Two guiding principles inform my understanding of deterrence theory.

---

[1] See, for instance, Alex Wilner, "Deterrence by Delegitimization in the Information Environment: Concept, Theory, and Practice," *Deterrence in the 21st Century: Statecraft in the Information Environment* (University of Calgary Press, 2024); Alex Wilner and Andreas Wenger (eds.) *Deterrence by Denial: Theory and Practice*, (Cambria Press, 2021); Alex Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies*, 43:2 (2020); Alex Wilner, "The Many Shades of Deterrence", *Policy Perspective*, Canadian Global Affairs Institute, August 2022; Alex Wilner and Casey Babb, "New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour," in *Deterrence in the 21st Century* (*Netherlands Annual Review of Military Studies 2020)*, Osinga and Sweijs (eds.), (Springer: 2021); Alex Wilner, *Deterring Rational Fanatics* (Philadelphia, PA: University of Pennsylvania Press, 2015); Andreas Wenger and Alex Wilner (eds.) *Deterring Terrorism: Theory and Practice* (Stanford University Press, 2012); Alex Wilner, "Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism," *Journal of Strategic Studies* 34:1, (2011): 3-37.

[2] Marshall Palmer and Alex Wilner, "Deterrence and Foreign Election Intervention: Securing Democracy through Punishment, Denial, and Delegitimization," *Journal of Global Security Studies* 9:2 (2024).

First, deterrence is not simply something that you say or casually lump together with other related terms, like 'defence, enforcement, or defeat'. Rather, **deterrence is a framework or strategy,** built on foundational theoretical principles about the nature of behaviour, that can be applied within any context in which we seek to counter or change another actor's behaviour.

And second, if deterrence is defined as convincing an adversary to forgo an unwanted action, then in practice deterrence isn't something that just happens naturally or on its own. Rather, **deterrence is something that you do and communicate**, proactively. Deterrence is the result of putting into practice a strategy that seeks to manipulate, shift, or change an adversary's behaviour in ways that meet our core objectives.

Several prerequisites inform the strengths and utility of any deterrence framework. First, deterrence involves at least two actors. The adversary – often labelled as the challenger by deterrence scholars – seeks to pursue an unwanted action. The challenger is the actor being deterred. The second actor – often referred to as the defender by scholars – seeks to convince the challenger not to engage with an unwanted action. The defender is the actor issuing a deterrent threat. Another way to think about these relations and outcomes is that challengers want to change a status quo relationship, while defenders seek to uphold it. In our case, **Canada is the defender**, and foreign actors contemplating interference are the challengers.

Second, when done right, a deterrence framework should seek to weigh on a challenger's **cost-benefit analysis**. Rational behaviour is predicated on the costs or effort an action is assumed to entail against the benefits or gains the action is assumed to generate. When a rational actor believes that the costs of its actions outweigh the perceived benefits, deterrence theory speculates that it should subsequently forgo a particular behaviour. Thus, as a prerequisite to deterrence, a challenger must be sufficiently swayed by rational choice.

Third, for deterrence to work as theorized, both the challenger and the defender must share a baseline preference for inaction under some conditions. If either or both seek to hurt the other above all else, then deterrence theory cannot function in practice.

Fourth, threats and expectations must be clearly **communicated** to a challenger, such that it can absorb relevant information, consider how to response, and inform or change its behaviour. Communication is critical to deterrence. A threat that is unmade or a warning that isn't heard or properly understood, will fail to generate the desired coercive effect of our challengers.

Fifth, defenders must have a perceived **capability** to act as they have threatened, and to demonstrate a resolve to act as threatened if and when required. Bluffing can undermine deterrence. A challenger must believe that a defender can and will act as it has communicated.

And finally, deterrence works best against a known adversary. Anonymity in either physical or digital space complicates how deterrence is communicated and carried out. **Attribution** is an important consideration when identifying and threatening our adversaries.

By putting all of these definitions, concepts, and prerequisites together within the context of deterring foreign interference in Canada, three deterrence pathways present themselves**: deterrence by punishment; deterrence by denial; and deterrence by delegitimization**.

Deterrence by punishment promises some form of retaliation if a challenger pursues an unwanted action (e.g., kinetic or cyber retaliation, sanctions, seizure, prosecution, etc.). Punishment adds to an adversary's costs, potentially tipping the scales of any cost-benefit calculation towards inaction.

Deterrence by denial, conversely, functions by subtracting from or diminishing an adversary's perceived benefits.[3] Here, our goal is to deny a challenger what it seeks. From a cost-benefit perspective, denial creates a cost by promising failure. If an adversary is convinced that the unwanted action in question is unlikely to get them what they desire, they may be less willing to try in the first place.

Deterrence by delegitimization – a new and normative approach to coercion that I first proposed in relation to deterring religiously-inspired terrorism and have since begun applying to information warfare[4] – functions by informing and shaping an adversary's beliefs, attitudes, ideologies, and other motivating forces. Delegitimization turns on social pressure and perceptions of right and wrong. Here, challengers are deterred from pursuing a certain behavior when the behavior itself generates a belief or perception within the actor or among its constituents, stakeholders, or supporters that pursuing the action would be shameful, disgraceful, and detrimental to their larger goals or objectives.

Recommendations:

I strongly encourage members of the commission to use the term 'deterrence' diligently and consistently to refer to a larger framework in which Canada leverages a combination of threats and defences to countering FI in a way that convinces actors who mean us harm *not* to pursue foreign interference and related activities. Deterring all FI is likely impossible; but deterring some actors from pursuing some forms of FI some of the time is entirely feasibly. Without a core strategic logic wedded to deterrence theory, Canada's approach to countering foreign interference risks remaining a patchwork of under-coordinated activities unmoored from any singular focus or guiding north star.

A Canadian deterrence framework for countering foreign interference should combine elements of all three deterrent processes. The framework would provide the conceptual backbone for combining the disparate approaches to counter-interference under one guiding conceptual rubric of deterrence. Moreover, the framework would tie the various approaches and practical solutions that Canada and other democracies are proposing, testing and applying to countering foreign interference within a larger, overarching strategy. The strategy itself could be broken down and applied to different actors involved in interference in different ways. State and non-state sponsors of foreign interference and Canadians, foreign nationals, and domestic organizations involved in its promotion can be punished. The effect interference is meant to have on Canadians, on our society, and on our democratic processes can be denied. And bolstering democratic norms, values,

---

[3] Wilner and Wenger (eds.) *Deterrence by Denial*, (Cambia, 2021).

[4] Jerry Mark Long and Alex Wilner, "Deterring an 'Army Whose Men Love Death': Delegitimizing al-Qaida," *International Security* 39:1 (2014); , Wilner, "Deterrence by Delegitimization in the Information Environment," in *Deterrence in the 21st Century*, Ouellet et. al., (University of Calgary Press, 2024).

principles, expectations, and institutions might delegitimize the acceptance or use of foreign interference among a variety of stakeholders, from elected officials to individual Canadian voters.

Let me conclude, then, with a scenario that breathes life into the proposed deterrence framework and strategy.

Heavy and open investments in Canada's ability to investigate, enforce, and criminally prosecute domestic and foreign individuals, organizations, or corporate entities promoting foreign interference in Canada would occur under public and journalistic scrutiny, maximizing Canadians' awareness of contemporary threats to our democracy while communicating to would-be challengers Canada's capability, willingness, and resolve to punish FI activities robustly. Concurrently, Canadian officials, working lock-stop with our democratic allies, could issue a more nuanced and credible series of threats to punish state sponsors of interference, including by threatening sanctions and public exposure, and, possibly, at the extreme end, by threatening military or cyber retaliation for interference deemed a threat to critical Canadian or allied infrastructure.

Elsewhere, applying a whole-of-society approach to countering interference would deny its purpose and diminish its utility. Here, different levels of government would work with the federal government to limit and constrict the intended effects of foreign interference by diminishing the scope and reach of disinformation, by encouraging or forcing private sector partners to scrub disinformation from their platforms, and by improving Canadian cybersecurity practices in ways that diminish the theft of sensitive information that might be repurposed to influence our elections and elected officials. And by way of public and formal education campaigns, Canadian society's ability to identify and ultimately ignore disinformation meant to interfere with our democratic processes can be strengthen, further contributing to overall denial efforts.

Finally, clearly and repeatedly discrediting foreign interference domestically and internationally as a disgraceful form of behaviour by championing democratic norms and institutions, might, among and within certain societies, including our own, create a social cost to participating in foreign interference. This is more than simply wishful thinking. If interference is widely interpreted as illegal and shameful, would-be local politicians at all levels of government may become less inclined to accept, invite, or welcome foreign interference on their behalf. Doing so would be counter to what they believe is just and expected of them.

In sum, criminal law is a necessary but not sufficient means of deterring foreign interference in Canada. Deterrence entails a complex interaction between different actors and processes that encourages a more nuanced understanding of our adversaries' cost–benefit calculations in deciding whether, when and how to interfere in Canada. Crucially, deterrence theory helps identify the tools, technologies, infrastructures, and processes needed to manipulate and shape our adversary's calculus and preferences by weighing on and utilizing punishment, denial, and delegitimization together.