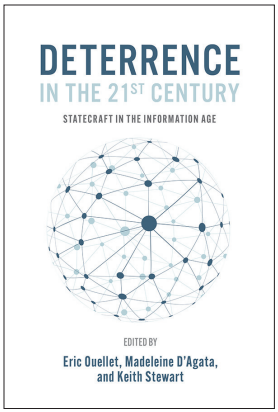
UNIVERSITY OF CALGARY
Press



DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

Introduction

Eric Ouellet[1]

It is no secret that Western democracies are facing significant challenges from Internet-based campaigns of disinformation conducted by various adversaries since the early 2000s. The People's Republic of China, Russia, and Iran have been pointed out on numerous occasions as key agents of disinformation, but we should also note that in North America, anti-liberal and anti-democratic domestic non-state actors are increasingly involved in active disinformation. These acts of disinformation have taken different forms such as spreading rumours about the origins of the COVID-19 virus or the war situation in Ukraine, revealing publically compromising private emails without context, organizing character-assassination campaigns against certain individuals, posting confusing information about electoral procedures, etc.

Such aggressions are not new, and in the past have been committed through various means of communication. They were quite common during the Cold War, when both official and secretive propaganda and rumour-spreading activities were organized by the West and the East. However, given the information technology revolution of the last few decades, the potential harm that disinformation could cause has reached unprecedented levels. As any society is ultimately built on trust in its institutions, and, given our greater reliance on information sharing through easily accessible technology, we find our economic, social, and political structures more vulnerable than ever to those who seek to sow confusion and discord. Furthermore, such vulnerabilities are increasingly becoming an arena for great power rivalry, where a political and strategic fracture between liberal democracies and non-liberal regimes is widening and becoming more apparent.

It is in this context that the Canada's Department of National Defence (DND) has been tasked with exploring new avenues to protect Canada, and

more generally North America, against disinformation. As an agency of DND, Defence Research and Development Canada (DRDC) launched a substantive research project seeking to evaluate if and how disinformation can be deterred in the twenty-first century. Hence, the title of this book, *Deterrence in the 21st Century: Statecraft in the Information Environment*. This book constitutes a first step in this research effort by providing the latest knowledge and thinking about how deterrence as a posture and disinformation as a threat can both conceptually and pragmatically inform policy, doctrine, and capability use and acquisition. This volume is the outcome of a call for papers sent in 2020 and 2021 that reached out broadly to academics, experts, and practitioners in Canada and abroad who have worked on new and emergent notions involving deterrence and disinformation to guide how we can fight back against disinformation and its consequences.

At the core of this book is the argument that the posture taken so far by the Canadian government and other Western states is mostly guided by inward-looking approaches, and that this is not sufficient to counter disinformation effectively. Concepts such as societal resilience build on reinforcing social justice, cohesion, and trust in key institutions through transparent and fair laws, policies, and programs, or information inoculation based on improving digital literacy and general civic education; each of these concepts focus on our societies' own vulnerabilities. Yet, disinformation involves adversaries who deliberately plan and implement activities in the information environment with malign intentions. Understanding their approaches and goals, and more importantly how their world views, prejudices, and deeply held preconceptions regarding Western societies frame their actions is equally important if one wants to be proactive in defeating disinformation. In other words, an outward-looking posture is also necessary.

This is where the concept of deterrence assumes its greatest importance. Any form of deterrence is built on understanding adversaries' strategies, tactics, goals, preferred approaches, and their assessment of their own strengths and of our own weak points, etc., so that we can pre-empt them from attacking by changing their calculus. In a deterrence posture, the other's mental world is the central focus. And yet, finer forms of deterrence require reflexivity. To this end, we must be critical of our own thinking about how our adversaries are construing us in order to avoid building our own preconceived notions into our assessment of these adversaries' world views. With this perspective

in mind, this book aims to shape the contours of what a deterrence posture against disinformation may look like.

Before presenting the various chapters of this book and their unique contributions to the understanding of disinformation deterrence in the contemporary world, it is useful to provide some conceptual definitions and clarifications, as research on deterrence and disinformation is still evolving in many different directions.

What Is Disinformation?

A first issue about disinformation that often leads to some confusion is that even if most of the twenty-first-century disinformation activities, as well as their countermeasures, are conducted using Internet-based information and communication technologies, they are not simply reducible to matters of technology. Automated computerized systems that create social media accounts and disseminate false information, or complex systems that identify narratives originally coming from dubious sources, for instance, are all part of the world of disinformation. Yet, what is actually believed by flesh-and-blood people and their actual behaviours that might ensue, the actual impact on policies and decision making, as examples, are the true stakes of disinformation and counter-disinformation. In other words, the cyber domain is a key enabler of today's world of disinformation, but it needs to be understood as a socio-political issue rather than a purely technological one. Disinformation, such as spreading rumours, is as old as humanity, and does not need advanced technology to be effective. The Soviet KGB of old is well-known to have developed disinformation almost to an art form, often referred to as "active measures" (Cull et al., 2017), which included activities such as creating front organizations to disseminate certain messages, recruiting and cultivating agents of influence in foreign countries, spreading fake stories in foreign media, and producing high-quality forgeries to sow confusion. Many of these types of activities are still seen today, but they are leveraging Internet-based technologies for dissemination.

Another issue is a matter of definition, as multiple terms, such as "fake news," "post-truth era," "information pollution," "alternative facts," "misinformation," or "disinformation," have been used to describe these new threats, which also creates some confusion. Recently, there seems to be some sort of consensus around "disinformation" being the most accurate one (Kapantai et al., 2020). One useful definition that incorporates both the notion of a wilful

attempt to create confusion and today's technological reality is "the purposeful distribution of fake, misleading, fabricated or manipulated content. These actors rely on 'computational propaganda'—or the use of automation, algorithms, and big data analytics—in order to influence or deceive social media users" (Bradshaw & Howard, 2021).

There are various techniques employed in putting forward disinformation campaigns, and some emerging typologies can be useful as well, especially in identifying and assessing how to respond to such disinformation (Kapantai et al., 2020). For instance, they include entirely fabricated stories and hoaxes, conspiracy theories built on existing beliefs, pseudo-scientific statements or even complete studies but with somewhat altered research results, partially true rumours, trolling (implanting incendiary comments) and posting excessively positive or negative reviews, biased analyses that may appear genuine, etc. Each of these generic forms of disinformation requires different countermeasures at the tactical level, but taken collectively they can be part of a larger strategic effort. Hence, another important distinction to keep in mind when discussing disinformation is the level of analysis, and whether it is approached from a tactical or strategic viewpoint.

The disinformation of today is also framed by the political, social, and economic constructs of the Internet-based realm. In particular, the increased use of privately owned web platforms, which are responding first and foremost to market logic rather than societal norms, has a number of quite negative consequences on matters such as data protection and privacy; controlling content for lies, hate speech, and subversive narratives; allowing foreign states and their proxies to use them for their own purposes, as well as local actors pursuing political objectives seeking to undermine democratic institutions (Salter et al., 2019). This particular context is probably the most challenging part of Western democracies' responses to disinformation, as regulating market-based firms on matters of social and political narrative content is essentially anathema to liberalism (Freelon & Wells, 2020). Not only does regulation find itself lagging behind new forms and techniques of disinformation, but many of the countermeasures, to remain within the rule of law, are also reactive and require painstaking analysis and research to prove lies, hoaxes, or true authorship. Furthermore, given the scope and amount of disinformation, countermeasures such as "reality checks" and "fact checking" put forward by legitimate news media outlets and various organizations in civil society simply cannot keep up with the pace (Tsfati et al., 2020, p. 158).

These ongoing twenty-first-century disinformation campaigns are often done or sponsored by states and politicized non-state actors aiming to undermine liberal democracies. When it comes to state actors, they see such a goal as being in their interest in achieving international dominance, while Western non-state actors consider liberal democracy bankrupt. Those two generic groups of actors can be seen as "objective allies" in disinformation, even if it appears that active collaboration between states and Western non-state actors seems to be quite limited, and usually driven by other factors like vague ideological sympathies, or mercenary purposes. Many of those disinformation attacks are opportunistic in nature and leverage short-term legitimate concerns, yet they can have a longer-term strategic impact through the ongoing erosion of trust. A recent example is the active disinformation on short-term issues such as the campaign put forward by the People's Republic of China and Russia to undermine public confidence in COVID-19 vaccines, as formally noted by the European Union (Emmott, 2021). However, there are greater concerns about the compounding and longer-lasting corroding effects of disinformation campaigns against democratic institutions with regards to the management of public health, protection of privacy, protection of basic freedom and liberties, etc. Trust in the liberal state and its various agencies could suffer a host of damages that are difficult to repair (Rini, 2019). Years of active disinformation certainly played an important role in the lead-up to the 2021 Capitol riot in the United States, an event that came dangerously close to a far-right attempt at a coup d'état. This example alone illustrates how much Canada has a vested interest in fighting disinformation from a wider North American perspective.

On the brighter side, however, several analysts note that resilience to disinformation within Western democracies is greater than it is often presented by various authors and think tanks (Humprecht et al., 2020). The most salient disinformation events are often short-lived and can be corrected by sound public communications. As well, some have also highlighted that the greatest threat might be in "distrusting trust." An exaggerated belief in the vulnerability of Western audiences could lead Western states to become less liberal over time in order to protect "truth" from their citizenries. In other words, according to some analysts the majority of citizens are in fact a lot less gullible than some experts and politicians believe, but in reacting by implementing state measures limiting freedom of expression these same citizens might become less trusting of their governments (Dobber et al., 2020). This can be

a dangerous vicious circle that ironically supports the objectives sought by anti-liberal disinformation actors.

Disinformation in Canada

In light of this broader context, Canada finds itself in a situation not that much different from that of other smaller democratic states. Academic research about disinformation against Canada is still limited at the present time. A search of the available literature using the terms "disinformation" and "Canada" yields less than fifty academic articles at the time of writing. Most research and publically released information tends to be events driven, with some notable exceptions (Jackson, 2018). In the wake of revelations about foreign interference in the 2016 US presidential election, several publications focusing on prevention and post-factum assessment of disinformation during the Canadian election of 2019 were produced from various sources: academia, government, think tanks, and news media (Dubois & McKelvey, 2019; Tenove, 2020; Tenove & Tworek, 2019). More recently, with revelations of the People's Republic of China's sustained disinformation activities regarding the origin of the SARS-CoV-2 pathogen, the focus once again moved, this time toward COVID-19-related disinformation (MacDonald et al., 2020).

Information about disinformation in Canada remains mostly in publications from governmental agencies, and essentially from the Canadian Security Intelligence Service's (CSIS) open publications. These documents present disinformation in Canada in general terms and offer limited material to work with. The *CSIS Public Report 2020*, for instance, states that

> While foreign interference conducted by hostile state actors and their proxies most often occurs in the form of human interaction, the manipulative activities of foreign entities on a range of online social media platforms are increasingly of concern. Most recently, such state-sponsored manipulation, including through disinformation, has sought to reshape or undermine certain narratives to sow doubt about the origins of the coronavirus and pandemic as well as the means required to counter it; discredit democratic responses to COVID-19 while casting their own responses as superior; and erode confidence in Canada's values of democracy and human rights. Russia and Russian Intelligence Services have, for example, been actively engaged

> in disinformation campaigns since March 2020 in an effort to blame the West for the COVID-19 pandemic. This is part of a broader campaign to discredit and create divisions in the West, promote Russia's influence abroad, and push for an end to Western sanctions (CSIS, 2020, p. 23).

This longer quote constitutes, in fact, all this report has to say about disinformation. This particular example shows that for the time being the Canadian government has not engaged its population to a significant degree on the risks and dangers that disinformation represents to the country's democratic and liberal institutions. If experts and bureaucrats inside the Canadian state are well aware of the issues at stake, monitor closely new developments, and propose measures built on constructive counter-narratives, a wider dialogue on where the country stands in this brave new world remains to be initiated.

The greater source of open information about disinformation in Canada remains for the time being in mainstream news media, and a few civilian organizations such as the University of Toronto's Citizen Lab. Most of the reporting in news media tends to emphasize particular disinformation attempts, such as the claim that Canada has opened quarantine concentration camps (Tasker, 2020), that a Quebec-based professor is an active agent of disinformation for Russia (Daigle, 2020), that India is engaged in disinformation against Canadians Sikhs ("WSO's report alleges," 2021), etc. In other cases, there are general concerns raised about disinformation in Canada (Andersen, 2021; Farber & Fishman, 2021; "Half of Canadians," 2021) or general comments about the annual publication of the CSIS report, with an emphasis on disinformation. The public message, however limited it might be, is that disinformation attempts in Canada are real and actively spread by both foreign and domestic agents of influence, but the overall impact remains unstated and un-assessed.

Civil organizations such as the University of Toronto Citizen Lab offer more elaborate analyses, and on a wide set of topics ranging from privacy concerns related to certain phone or computer applications, to proposed legal changes, to the role of foreign firms in the upcoming implementation of 5G networks, to name just a few. Similarly, the NATO Association of Canada has created a Centre for Disinformation Studies presenting various research analyses on disinformation in social media, how Russia is using it, how the People's Republic of China's control over information is aligned with its

disinformation campaign, etc. Although these organizations provide more in-depth research on various facets of disinformation, much of this output nonetheless fails to assess the actual scope and impact of disinformation in Canada.

A few recent studies have been published, especially in the context of the COVID-19 pandemic, that are more empirical in nature. These studies have examined beliefs in conspiracy theories in Canada, and one in particular is focused on theories about the non-natural origins of the virus, and which seem to have been embraced by a substantive number of Canadians ("Significant minority," 2021), but such results and methodologies are questionable. The Biden administration in the United States and many other governments have been questioning the World Health Organization's findings about the origins of the virus, and as noted in a detailed analysis in the *Bulletin of the Atomic Scientists*, Western journalists have uncritically swallowed dubious explanations from people linked to the Chinese regime, and by doing so have unwittingly spread disinformation. In many ways, the average Canadian seems wiser than pollsters.

Other research involved assessing whether racist acts, especially toward Asians, are on the rise in Canada (Chinese Canadian National Council Toronto Chapter, 2021), and the role of far-right disinformation has been highlighted. However, the actual causal relationship between disinformation and such racist acts is implied rather than demonstrated. As well, the possibility that Beijing-led disinformation aimed at fostering anti-Asian feelings in order to create (perversely) more sympathy for its propaganda is also not addressed. Hence, there is a general sense that Canada is indeed impacted by disinformation, and it appears to lead to reprehensible behaviours in some instances, but the overall picture is not clear. As noted before, disinformation in Canada seems mostly a tactical and opportunistic tool that exploits existing tensions and events, while the overall strategy appears to be limited to undermining social institutions in Western liberal democracies as a general and undefined goal.

In the face of such a threat, the Canadian government has not remained idle, but the response has been mostly reactive and fragmented, or kept under the wrap of secrecy. In the wake of the Canadian election of 2019, a number of initiatives were put in place by various levels of government. With respect to the federal government, awareness campaigns such as Get Cyber Safe and the Digital Citizen Initiative were launched with modest budgets. An inter-agency

group, the Security and Intelligence Threats to Elections (SITE) Task Force, was also created. SITE comprised individuals from CSIS, the Royal Canadian Mounted Police, Global Affairs Canada, and the Communications Security Establishment (CSE). Several departments, such as National Defence, Global Affairs, and the Privy Council, have created informal, formal, and technical study and policy groups to deal with disinformation activities from both domestic sources and foreign, state-sponsored ones. These study and policy groups have had a renewed impetus with the disinformation campaigns that were observed since the beginning of the COVID-19 pandemic.

Canada and Defence's Reaction to Disinformation

In 2020 the federal government proposed a comprehensive umbrella policy under the name the Digital Charter, aiming at the entire Internet domain, including, among other areas, broadband access, online payment transparency and standards, the development of a digitally skilled workforce, hacking and cyber-attacks, information protection and privacy, quantum computing, and disinformation. The charter was closely associated with Bill C-11 to enact the *Consumer Privacy Protection Act* and the *Personal Information and Data Protection Tribunal Act*. The charter, although providing a global view of what the Canadian government does in the information environment, remains a patchwork of initiatives, legislation, and policies from numerous government departments and agencies. This fragmentation has also been noted by observers and academics (Bereskin, 2020; Kolga, 2021), who have highlighted that Canada lacks a clear and unified strategy to tackle disinformation, be it homegrown or from foreign powers such as the People's Republic of China, Russia, and Iran.

Within the Government of Canada, National Defence and the Canadian Armed Forces have been at the forefront of thinking about the threat that disinformation represents for many years now. However, the challenge for Defence is that although it can support other departments, such as the CSE, which is protecting the Government of Canada's information infrastructure, unless it is linked to a military or defence matter, its capacity to lead and implement solutions is limited. Defence's Public Affairs has developed various communication strategies to deal with disinformation. These strategies are not publically available, but they are not fundamentally different from similar public relations strategies found in other governmental organizations. On the more proactive side, DND found itself in a quite embarrassing, if not

scandalous, situation during the COVID-19 pandemic, as it put in place a plan to fight disinformation domestically that invoked phrases like "information operations," "shaping and exploiting information," etc. (Pugliese, 2020). Using conventional military terminology, and putatively accompanied by an operational mindset, the military was seen as aiming to influence legitimate Canadian media and sources of information, something that has been construed as a potential serious breach of trust and a threat to the concept of democratic civil control over the military. Although the Canadian military's intentions were very far from being disloyal to the civilian leadership, and these were essentially actions from a few overzealous staff officers, if anything, this event highlights a substantive lack of strategic-level maturity within defence circles about the nature and risks of domestic disinformation, and how to deal with it.

On the international front, DND has performed better. The Canadian leadership and substantive deployment in the NATO Enhanced Forward Presence (EFP) in Latvia has been the target of numerous Russian attempts at discrediting the mission, especially in the eyes of Russian-speakers in Latvia. Some of those attempts were quite naive and thus easily dismissed, such as media campaigns about the "gay Canadian battalion" using file pictures of the ex-colonel and convicted rapist and murderer Russell Williams in women's underwear (Brown, 2017). Yet, other attempts are more subtle and more concerning. More recently, in 2020, there were claims that the Canadian contingent was infecting the Latvian population with COVID-19 (Brewster, 2020). Similarly, during a different mission, conducted in the summer of 2019, a Ukrainian online magazine published the names of several Canadian military trainers engaged in the Canadian assistance mission in that country, declaring them mercenaries of the United States. The names were classified to protect the individuals from personal attacks.

The Canadian military in Latvia has developed a fairly sophisticated approach to deal with disinformation that is in line with the whole-of-government philosophy, involving the Canadian embassy, Global Affairs Canada in Ottawa, governments of other nations that are part of the Latvia's EFP, the Latvian government, as well as local Latvian stakeholders. The response to disinformation is managed through a strategic communication cell within the Canadian EFP headquarters. The cell not only monitors developments in various media, but also develops a strategic outlook focusing on areas that Russian-backed disinformers are likely to target, based on various

socio-demographic analyses and surveys done by the Latvian government. The cell also identifies proactive measures to build confidence and resilience against disinformation with local Latvian populations, ranging from organizing or participating in public events and fairs, organizing guest lectures in local schools about the mission, maintaining an open-minded approach with Latvian journalists, etc. Hence, in an expeditionary context at the tactical and operational levels, National Defence and the Armed Forces have shown a substantive capacity to deal with disinformation, and they continue to develop and refine ways and processes to do so.[2]

Deterrence against Disinformation as a Strategic Posture for Canada

Based on the above, it is clear that Canada is missing a strategic and comprehensive policy approach to disinformation that would help in creating synergies and greater effectiveness among disjointed capabilities and organizations. It is in this context that the notion of deterrence as a holistic posture against disinformation has emerged as a possible way forward.

DND, in conjunction with Global Affairs Canada, is now looking at deterrence as a deliberate way for Canada to address disinformation more strategically, and some internal initiatives in this regard have already begun. One such initiative is led by DRDC under the wider research portfolio of the Defence of North America, the goal of which is to explore what disinformation deterrence might mean for Canada. This initiative is looking at various questions, such as what this posture might look like, whether it is even feasible, what kind of technological requirements it would entail, DND's potential role, etc. The notion of disinformation deterrence is also being explored by some key allies of Canada, particularly the United States and several NATO countries.

A first challenge, however, is the fact that the notion of deterrence has itself been inherited from both conventional military posturing of old, and from the nuclear deterrence of the Cold War through such strategies as mutually assured destruction. Classic deterrence plays very much on the notion of fear—fear of our strengths and resilience, fear of our resolve and will; each of these support deterrence, but mostly in its retaliatory version. Another important aspect of classical thinking about deterrence is that it was understood as a dialogue of sorts, in which the various parties implicitly agree to engage. During the Cold War, each superpower made it clear where the "red lines" were, and boasted publicly of their respective nuclear capabilities should an

adversary decide to cross such lines. The Cuban Missile Crisis became a crisis in part because the Soviet side hid its threatening nuclear capabilities, and so the Kennedy administration had no choice but to publicly declare a new set of "red lines" supported by a clear show of force. The so-called red phone that was implemented afterward, to avoid future misunderstandings, speaks quite eloquently to this notion of deterrence as a dialogue.

Since the end of the Cold War, debates and discussions about deterrence have evolved and new notions and concepts have emerged. The problem is that new adversaries were not interested in such a dialogue and had very little to lose, and therefore it was not possible to play on their fears. Even before the events of 9/11, there were already significant concerns that a state, and then non-state actors, would use weapons of mass destruction (WMD) based on chemical, biological, and/or radiological compounds against civilian targets, and that the old rules of nuclear deterrence between the superpowers no longer applied. Attack attribution can be very well concealed and hard to prove, and many authoritarian regimes seem not to care if their own population pays a price for their misdeeds if deterrence by retaliation or punishment is implemented. For instance, Saddam Hussein's Iraq faced a massive embargo for several years as a result of the government's WMD programs during the 1990s, and yet they did not try to come clean about their efforts, even if they eventually dismantled those programs. Then, the so-called war on terror brought to light new threats and challenges, with the fear that terrorist organizations might use various forms of attacks, including potentially nuclear bombs, and it would be even harder to determine clear or specific targets for retaliation. Accordingly, deterrence appeared at some points nearly impossible against such ghostly adversaries.

Various analysts then came up with revamped notions such as deterrence by denial, whereby an adversary, rather than be deterred by the threat of massive retaliation—fear being a key factor in such calculations—would instead be brought to the point where they would consider continued threats and attacks against their Western enemies utterly futile (Edwards, 2011; Smith & Taylor, 2008). Concretely, this meant a combination of passive measures, such as the additional security protocols introduced in airports, at borders crossings, in financial transaction tracking systems, greater surveillance capabilities, etc., and active measures such as targeted assassinations of terrorist leaders, the seizure of suspicious sea shipments, de-radicalization programs in correctional facilities and socio-economically disadvantaged neighbourhoods, etc.

Another form of deterrence discussed in the post–Cold War era was deterrence by de-legitimization (Wilner, 2011). If it is true that terrorist organizations can hide in a population and do not usually defend a particular piece of territory, they are still reliant on support from various populations and networks abroad. Such support takes many forms, such as money, equipment, transportation, intelligence, the provision of safe houses for people and caches for weapons and equipment, the recruiting of new volunteers, etc. Hence, terrorist organizations, while they cannot be engaged in a deterrence dialogue, can be cut off from their support networks, thereby significantly hampering their capacity to operate, through the de-legitimization of their goals, their policies, their methods, etc. Furthermore, by improving local governance and the socio-economic conditions of their supporters, the allure these terrorist organizations are able to exert would be undermined. In a way, this form of deterrence is about establishing a positive and constructive new deterrence dialogue with the backers, rather the adversaries themselves.

In today's world of fake news, alternative facts, and disinformation more generally, deterrence again has been assessed and discussed as a policy, strategy, and/or state posture. Some elements of deterrence show certain similarities with the effort to deter terrorists and insurgents. Many disinformers hide among the population, and they cover their tracks through various forms of technological sophistication. They have very limited assets that could be leveraged for deterrence by retaliation. The links between them and their state backers, if they do have backers, are tenuous and difficult to prove. However, they present some new aspects, or at least characteristics that are more pronounced, if compared to terrorists and insurgents.

First, contrary to foreign insurgencies, today's disinformers are acting directly on Western populations' opinions and beliefs, and yet they do so not to help their own national cause, but rather to undermine liberal state institutions in the West, an effort that is oftentimes construed as an end in itself. As well, they do have "objective allies" in the West in groups opposed to liberalism, in the Far Left but mostly in the Far Right, and in radicalized and disaffected segments of the population. If once upon a time Ho Chi Minh stated that the solution of the Indochina problem was in France's domestic opinion, we now face a quite different dynamic. It is about undermining the West from within itself, as an end in itself. In a sense, the deterrence dialogue seems to have shifted once again to focus on the West's own population rather than on adversaries or their backers.

A second aspect is that disinformers, even the ones acting directly on the behalf of a foreign state, do not depend on any particular population to support them, and hence they have little to no legitimacy or reputation to lose. Deterrence by de-legitimization therefore becomes that much harder to implement, but it is not necessarily impossible. Of course, pressures could be applied against foreign states through economic and diplomatic sanctions, and even possibly by humiliating them through public exposure, in ways comparable to the United States showing pictures of Soviet missile launch sites being prepared during the Cuban Missile Crisis of the early 1960s. The numerous and open discussions in the Western news media about the active involvement of the People's Republic of China in spreading disinformation about COVID-19 have shown that disinformation can seriously backfire if publicly exposed (Verma, 2020).

A third, somewhat ironic aspect is that nuclear deterrence is also coming back to the forefront. A number of analysts have identified the potential risk that disinformation could create so much confusion and uncertainty that a conventional attack that crosses a "red line" for nuclear retaliation would remain unpunished because of our inability to justify a robust response due to disinformation. Hence, this has the potential to nullify nuclear deterrence, as the resulting confusion would not allow for a normal deterrence dialogue. The Russian government, in its 2022 military invasion of Ukraine, has already tried this very approach, but with limited success as Western powers were able to uphold a united front. Future crises in and around Taiwan have the potential to lead to a similar scenario.

If we go back to Canada's policy in this rapidly evolving world, difficult questions are thus raised. What would disinformation deterrence look like, and what would be the effective mechanisms to play on adversaries' fears? From a technical standpoint, what new capabilities should be developed? How far should we go in developing capabilities based on a mixture of cyber technology, intelligence gathering, communication studies, and social sciences solutions? Canada could somehow copy the old Russian and Soviet playbook of developing culturally sensitive *kompromat* against adversaries' senior leadership, for instance? How realistic these options are remains to be assessed. The country has a long tradition of trying to keep its adversaries at bay by various means that do not involve direct coercion, preferring instead for others like the United States to do so while benefitting from its close relationship with its southern ally. Also, Canada's historical preference is to act

only as part of a wider concerted effort when it comes to engaging in more coercive solutions. What others will do is likely to weigh heavily on our future policies. Finally, there are risks that adversaries might pay more attention to Canada. Some Canadian politicians, for instance, could possibly be seriously embarrassed if actively targeted by concerted actions from foreign actors, thereby undermining their capacity to govern. In other words, adversaries may choose to retaliate in kind against Canada more often if we implement a posture of deterrence by punishment. In the end, we may ourselves be deterred from responding to disinformation as a result of fear.

This brings us to the more practical and politically acceptable posture of deterrence by denial, but this also implies that the Canadian government will have to be much more upfront with the public by presenting the threats of disinformation with greater insistence. This also means naming our adversaries and seeking to understand and acknowledge their politically, socially, culturally, and psychologically malign inclinations toward us. The publication of the Canadian Indo-Pacific Strategy in 2022, in which the People's Republic of China is described as a "disruptive global power," constitutes a first step in that direction. Yet, powerful institutional traditions remain. For a long time, successive Canadian governments have chosen as a matter of policy mostly to keep the public in the dark with respect to the nature of the threats against the country, and their degree of intensity. This has been termed an "Alice in Wonderland" attitude (Potter, 2010). In the end, any change in Canada's strategic approach to disinformation is likely to also require a critical and self-reflexive change in its strategic culture implicitly built around the belief that we are somehow remote from the world's problems.

Structure of the Book

To provide some answers to these questions and many more, and to introduce new ideas, notions, and techniques linked to fighting disinformation, this book has been divided into four major sections. The first section, "Deterrence as an Evolving Concept," is made up of three chapters, which look deeper into the origins and the implications of deterrence as a concept to guide policy and ultimately actions against Canada's adversaries. The first chapter, from Christopher Ankersen of New York University, provides further useful definitions, and explores the assumptions implied in classical deterrence by punishment and its focus on cost-benefit analysis. The second chapter, from Stephen Cimbala and Adam Lowther, both from the US Army Staff

College, discusses the notion of time in the context of deterrence, which has been significantly compressed by the massive implementation of information technology, allowing for real-time (dis)information and thus framing how deterrence could be implemented. The last chapter in this section, by Alex Wilner of Carleton University, re-engages us in the concept of deterrence by de-legitimization, which was originally introduced in dealing with the difficult context of fighting insurgencies and terrorism.

The following section, "Wider Strategic Context and Experiences," looks into both the external origins of the disinformation threat, especially from Russia and the People's Republic of China, and the experience of Israel in dealing with the complexities of putting together a credible deterrence while dealing with disinformation. The first chapter is by Rachel Lea Heide, from Defence Research and Development Canada, and presents the more salient aspects of the disinformation techniques and approaches used by Russia. This chapter is followed by a contribution from Anthony Seaboyer and Pierre Jolicoeur of the Royal Military College of Canada discussing how the People's Republic of China is actively using disinformation to achieve its strategic political objectives. Moving from adversaries to democratic nations having to deal with both deterrence and disinformation, the chapter by Ron Schleifer and Yair Ansbacher looks into the complex situation of Israel, which since its founding had to develop a credible and comprehensive deterrence posture against nation-states, but which in the last two decades has evolved in the direction of dealing with non-state adversaries such as Hamas and Hezbollah. Concluding this section, and extending the analysis from the previous chapter, Oshri Bar-Gil of the Israel Defense Forces' Applied Behavioral Science Institute presents Israel's own perspective on what constitute disinformation and how it applies to the country's situation in the Middle East. In particular, Bar-Gil highlights the challenges stemming from the asymmetric nature of disinformation and seeks to understand how deterring disinformation requires a change in mindset, away from classical deterrence, in order to be effective.

The third section, "Canada's Context," emphasizes not only the actual risks involved in being a target of disinformation, but also where our thinking and practices should focus when it comes to dealing with disinformation, and more generally where we stand in terms of our deterrence capabilities. The first chapter here comes from Nicole Jackson of Simon Fraser University. Extending the reflections emerging from the previous chapters

to the particular case of Canada, Jackson proposes a refined analysis of what disinformation and deterrence could potentially mean. The second and last chapter in this section is provided by Christian Leuprecht of the Royal Military College of Canada and Joseph Szeman of Queen's University. These authors extend the reflection proposed in the previous chapter and highlight the fact that Canada has been somewhat behind the new thinking about disinformation and deterrence, which has in turn impacted our choice of policies and strategic posture, especially in light of the synergistic relationships between the cyber and informational domains.

The fourth and last section, "Emerging Tools and Approaches," is made up of three chapters that highlight and describe some emerging concepts, methodologies, and cautionary warnings to support the development of a sound deterrence posture against disinformation. The first is by Sarah Jane Meharg, of the Canadian Forces College, and explores the notion of digital tribalism. If it is clear that disinformers play on groups' feelings to motivate them to oppose liberal democratic institutions, and that older notions such as right- and left-wing populism or nationalism are becoming less useful in understanding some of the underlying dynamics of group behaviour. The next chapter, by Anne Speckhard and Molly Ellenberg of the International Center for the Study of Violent Extremism, looks into how counter-radicalization efforts can support deterrence by denial in offering credible and emotionally engaging counter-narratives tailor-made to the socio-economic and cultural realities of potential recruits. This chapter is followed by the by contribution of Ronald D. Porter (Saint Mary's University), Minqian Shen (Queen's University), Leandre R. Fabrigar (Queen's University), and Anthony Seaboyer (Royal Military College of Canada). The authors review the various methodologies available to assess indirectly how a particular audience might have been influenced by online communication, and especially disinformation.

The concluding chapter is from Keith Stewart and Madeleine D'Agata, of Defence Research and Development Canada. They propose, in light of the previous chapters, a series of reflections and some high-level conclusions from the diverse material offered throughout the book. In particular, they argue that the changing context requires a refreshing of our knowledge of, and techniques for, understanding and influencing a diversity of adversaries with an emphasis on achieving a posture based on deterrence by denial.

NOTES

1 Some portions of this chapter were previously published in Ann Fitzgerald and Craig Stone (Eds.), *Managing security and defence in the 2020s: The post-pandemic challenges*, Breakout Education, 2023.

2 This information about the Canadian EFP measures against disinformation has been provided by an expert military source who prefers to remain anonymous.

REFERENCES

Andersen, R. (2021, 26 March). Social media platforms pressured to remove accounts spreading COVID-19 disinformation. *CTV News*. https://www.ctvnews.ca/health/coronavirus/social-media-platforms-pressured-to-remove-accounts-spreading-covid-19-disinformation-1.5364495

Bereskin, C. (2021, 21 May). Should Canada adopt an anti-"fake news" law? *NATO Association of Canada*. https://natoassociation.ca/should-canada-adopt-an-anti-fake-news-law/

Bradshaw, S., & Howard P. N. (2018, 17 September). The global organization of social media disinformation campaigns. *Journal of International Affairs*. https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns

Brewster, M. (2020, 24 May). Canadian-led NATO battlegroup in Latvia targeted by pandemic disinformation campaign. *CBC News*. https://www.cbc.ca/news/politics/nato-latvia-battle-group-pandemic-covid-coronavirus-disinformation-russia-1.5581248

Brown, C. (2017, 16 June). Anti-Canada propaganda greets troops in Latvia. *CBC News*. https://www.cbc.ca/news/world/latvia-propaganda-1.4162612

Chinese Canadian National Council Toronto Chapter. (2021). *A year of racist attacks: Anti-Asian racism across Canada: One year into the Covid-19 pandemic*. Chinese Canadian National Council Toronto Chapter.

Cull, N. J., Gatov, V., Pomerantsev, P., Applebaum, A., & Shawcross, A. (2017). Soviet subversion, disinformation and propaganda: How the West fought against it: An analytic history, with lessons for the present. *LSE Consulting Report*. LSE School of Global Affairs.

CSIS (Canadian Security Intelligence Service). (2020). *CSIS Public Report 2020*. Government of Canada.

Daigle, T. (2020, 21 October). Canadian professor's website helps Russia spread disinformation, says U.S. State Department. *CBC News*. https://www.cbc.ca/news/science/russian-disinformation-global-research-website-1.5767208

Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *International Journal of Press/Politics, 26*(1), 69–91. https://doi.org/10.1177/1940161220944364

Dubois, E., & McKelvey, F. (2019). Political bots: Disrupting Canada's democracy. *Canadian Journal of Communication Policy Portal, 44*, 27–33. http://doi.org/10.22230/cjc.2019v42n2a3511

Edwards, A. (2011). Deterrence, coercion and brute force in asymmetric conflict: The role of the military instrument in resolving the Northern Ireland "Troubles." *Dynamics of Asymmetric Conflict, 4*(3), 226–41.

Emmott, R. (2021, 29 April). Russia, China sow disinformation to undermine trust in Western vaccines: EU. *Reuters*. https://www.reuters.com/world/china/russia-china-sow-disinformation-undermine-trust-western-vaccines-eu-report-says-2021-04-28/

Farber, B., & Fisman, D. (2021, 14 May). The overlap between lockdown agitators and hate groups is a threat to us all. *Globe and Mail*. https://www.theglobeandmail.com/opinion/article-the-overlap-between-lockdown-agitators-and-hate-groups-is-a-threat-to/

Freelon, D., Wells, C. (2020). Disinformation as political communication. *Political Communication, 37*(2), 145–56. https://doi.org/10.1080/10584609.2020.1723755

Half of Canadians regularly receive fake news through private messaging apps. (2021, 11 May). *The Suburban*. https://www.thesuburban.com/life/lifestyles/half-of-canadians-regularly-receive-fake-news-through-private-messaging-apps/article_ded65b20-b289-11eb-983d-6b1c0dfd30a1.html

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *International Journal of Press/Politics, 25*(3), 493–516. https://doi.org/10.1177/1940161219900126

Jackson, N. J. (2018). Canada, NATO, and global Russia. *International Journal, 73*(2), 317–25. https://doi.org/10.1177/0020702018786080

Kapantai, E., Christopoulou, A., Berberidis, C., & Peristeras, V. (2020). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society, 23*(5), 1–26. https://doi.org/10.1177/1461444820959296

Kolga, M. (2021, February). Taiwan demonstrates how we can defend Canadian democracy against information warfare. *Policy Perspective Calgary*. Canadian Global Affairs Institute. https://www.cgai.ca/taiwan_demonstrates_how_we_can_defend_canadian_democracy_against_information_warfare

MacDonald, N. E., Comeau, J., Dubé, E., Bucci, L., & Graham, J. E. (2020). A public health timeline to prepare for COVID-19 vaccines in Canada. *Canadian Journal of Public Health, 111*(6), 945–52. https://doi.org/10.17269/s41997-020-00423-1

Potter, M. (2010, 29 November). Canada has "Alice in Wonderland" attitude on terrorism: Wikileaks. *Toronto Star*. https://www.thestar.com/news/world/2010/11/29/canada_has_alice_in_wonderland_attitude_on_terrorism_wikileaks.html

Pugliese, D. (2020, 21 July). Canadian Forces "information operations" pandemic campaign quashed after details revealed to top general. *Ottawa Citizen*. https://ottawacitizen.com/news/national/defence-watch/canadian-forces-information-operations-pandemic-campaign-squashed-after-details-revealed-to-top-general

Rini, R. (2019). Social media disinformation and the security threat to democratic legitimacy. In Joseph McQuade (Ed.), *Disinformation and digital democracies in the 21st century* (pp. 10–14). NATO Association of Canada.

Salter, L., Kuehn, K., Berentson-Shaw, J., & Elliot, M. (2019). Literature review part 1: Threats and opportunities. *Digital threats to democracy*.. https://static1.squarespace.com/static/5cbe92fcaf4683f10f6c8de5/t/5cd11bb67817f7493acb89be/1557207991882/3.DD-background-paper-lit-review-1-WEB.pdf

Significant minority of Canadians believe COVID-19 misinformation, rivalling long-established conspiracy theories. (2021, 30 April) *InsightWest*. Retrieved 10 May 2021 from https://www.insightswest.com/news/conspiracy-april-2021/

Smith, J., & Talbot, B. (2008). Terrorism and deterrence by denial. In P. Viotti, M. Opheim, & N. Bowen (Eds.), *Terrorism and homeland security: Thinking strategically about policy* (pp. 53–68). CRC Press.

Tasker, J. P. (2020, 20 October). PM, health officials warn Canadians against believing COVID-19 "internment camps" disinformation. *CBC News*. https://www.cbc.ca/news/politics/covid-19-internment-camps-disinformation-1.5769592

Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *International Journal of Press/Politics, 25*(3), 517–37. https://doi.org/10.1177/1940161220918740

Tenove, C., & Tworek, H. J. S. (2019). Online disinformation and harmful speech: Dangers for democratic participation and possible policy responses. *Journal of Parliamentary & Political Law, 13*, 215–32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3613166

Tsfati, Y., Boomgaarden, H. G., Strömbäck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis. *Annals of the International Communication Association, 44*(2), 157–73. https://doi.org/10.1080/23808985.2020.1759443

Verma, R. (2020). China's diplomacy and changing the COVID-19 narrative. *International Journal, 75*(2), 248–58. https://doi.org/10.1177/0020702020930054

Wilner, A. S. (2011). Deterring the undeterrable: Coercion, denial, and delegitimization in counterterrorism. *Journal of Strategic Studies, 34*(1), 3–37. https://doi.org/10.1080/01402390.2011.541760

WSO's report alleges Indian disinformation campaign against Canadian Sikhs. (2021, 3 February). *Online Voice*. https://voiceonline.com/wsos-report-alleges-indian-disinformation-campaign-against-canadian-sikhs/