CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

The Rise and Fall of Military Strategic Communications at National Defence 2015-2021:
A Cautionary Tale for Canada and NATO, and a Roadmap for Reform

by Brett Boudreau

May 2022

POLICY PAPER

THE RISE AND FALL OF MILITARY STRATEGIC COMMUNICATIONS AT NATIONAL DEFENCE 2015-2021: A CAUTIONARY TALE FOR CANADA AND NATO, AND A ROADMAP FOR REFORM

by Brett Boudreau

CGAI Fellow
May 2022

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-241-1

Contents

Executive Summary

On November 2, 2020, the Ottawa Citizen ran the front-page headline "Canadian Military Wants to Establish New Organization to Use Propaganda and Other Techniques to Influence Canadians." This seemed an unbelievable story, and one initially denied by a spokesperson for the minister of National Defence. Just three days later, though, then-chief of the Defence Staff (CDS) Gen. Jonathan Vance shuttered the group in question, terminating an initiative more than five years in the making that called into question the Department of National Defence's (DND) commitment to objective and appropriate public communication, at a time when truth decay, misinformation and disinformation have gained much traction around the world and in Canada.

In June 2021, the day Parliament adjourned for the summer, DND acknowledged to select media that acting CDS Lt.-Gen. Wayne Eyre and then-deputy minister Jody Thomas had determined the initiative was "incompatible" with government communications policy and the vision, mission and principles of DND Public Affairs. In a surprising self-indictment, the leaders also admitted a lack of "institution-wide strategic level direction and guidance," to build information-related capabilities that were "governed by appropriate authorities and oversight."

Deliberate influence campaigns by malign state, non-state and increasingly by domestic actors to disturb, disrupt and create disorder in democratic societies have become widespread and commonplace. The volume of vitriol is increasing. This is fast eroding citizen faith, trust and confidence in government and public institutions and may be the greatest contemporary threat liberal democracies face – arresting this trend and then restoring trust, the ultimate challenge. National Defence's entire program – to be successful on operations; secure sufficient funding; recruit, train and retain; effect culture change; reconstitute the force post-pandemic and procure the equipment needed to contest, confront and defeat adversaries – will largely depend on whether the institution can modernize its approach to strategic communications to manoeuvre more agilely and to better effect in a complex, frenetic and hostile information environment.

Recently, National Defence has suffered a significant self-inflicted setback in that regard. This monograph explains the rationale for, evolution of and factors behind the failure of the controversial Military Strategic Communications (MilStratCom) initiative: 10 lessons are identified and 20 recommendations suggested for how to recover lost ground and momentum. The initiative sought to create a new planning framework to more effectively co-ordinate everything the DND/Canadian Armed Forces (CAF) deliberately says, does and signals and thus communicates, to influence target audiences abroad or at home. That is a seriously ambitious undertaking, referring to all the means to inform, influence and persuade people (such as Public Affairs, information operations and psychological operations); actions (such as where the Royal Canadian Navy (RCN) sends a frigate or where the army trains, which communicates

something to someone, somewhere); and tools to coerce behavioural change (like bombs, bullets and missiles) or to deceive adversaries (deception operations).

However, ambiguous policies, troubling aspects of military culture and poor organization of effort established conditions that did not sufficiently guard against the prospect for unauthorized adventurism by practitioners to try to achieve desired effects favourable to the DND/CAF. As one rear admiral explained to the media, "the young folks we have that are keen on this sort of understanding the information sphere and then using those sorts of tools … we don't restrain that sort of initiative." This mindset also led to attacks by senior Public Affairs officers, tacitly sanctioned by senior leadership, against critics of Defence to try to influence media coverage. The strategy inevitably led to public missteps that negatively affected organizational credibility and institutional reputation. This was wilful negligence by DND/CAF leadership, military practitioner hubris and communications malpractice.

The good news is that DND/CAF has explained in internal reports how missteps occurred and has set in place some corrective measures. The bad news is that operator culture and mindset in certain quarters evidence a contemptuous attitude to direction by superior HQs, disdain for civilian authority and an allergy to external advice, which all remain entrenched. The ugly news is the recent off-the-charts operational tempo and overload of big issues happening concurrently means capacity and capability to take on new pan-institutional reform efforts are at a historic low. Of interest is whether appropriate lessons were learned to avoid a repeat performance or if the same approach, process, policies, doctrine, structure, governance, mindset and culture are still at play (spoiler alert: it's the latter).

Events like Brexit, the U.S. presidential elections of 2016 and 2020 – plus the latter's aftermath – the COVID-19 pandemic, the "freedom" trucker convoys and Russia's invasion(s) of Ukraine have one thing in common – the pernicious effect of mis- and disinformation. These momentous events demonstrate the critical need for superb leadership-enabled government communications capability and capacity. Re-imagining Defence communications to ensure institutional credibility and organizational reputation is a national security issue of the first order and for the DND/CAF, arguably an existential requirement. The need is for an enterprise-wide, joint, integrated military/civilian capability with skilled practitioners operating with fit-for-purpose policies, appropriate authorities, effective governance and real oversight to support domestic and overseas operations up to and including combat. Ideally, that effort would be nested within a broader government communications reform undertaking. Much is riding on being able to orchestrate a deliberate and demonstrably better effort in the next iteration of Defence communications reform.

Three Key Recommendations

- *This is a complex project and should be treated, organized and staffed like one. Create a defence communications task force with full-time DND/CAF representation of subject matter experts from the related disciplines and staff functions to hyper-accelerate the necessary policy, regulation, force development and training changes needed.*

- *Conduct a review of the Public Affairs group with its nearly 1,000 staff to find where long-standing conventions of organization structure need to change to improve outcomes and to strengthen the ability of the responsible authority to manage that function.*

- *Re-imagine the Defence communications capability enterprise-wide. Create an operational communications sub-classification and qualification course for officers and non-commissioned members in the regular and reserve forces. Make this a joint course, and a joint capability to replace the current information operations, psychological operations and influence activities model – one made for a pre-internet world – with a structure and approach that is purpose-built for the needs and demands of today's information environment.*

I: Introduction

"It is clear that the development of the various information related capabilities have suffered from a lack of institution-wide strategic level direction and guidance to grow a joint CAF and integrated DND/CAF capability that is professionalized, sustainable, and governed by appropriate authorities and oversight." [1]

Canadians expect, and policy compels, that the Department of National Defence (DND) and the Canadian Armed Forces (CAF) will be truthful in their public communications, following well-established practice consistent with democratic values and civilian control of the military. One caveat: during contested operations such as fighting alongside NATO in Afghanistan or with coalition forces against Daesh in the Middle East, Canadians accept that their military will use assets, tools and techniques to influence, coerce and deceive adversaries to protect our forces and those of our allies, and to be successful in battle. In situations of confrontation but less-than-open-conflict, such as NATO's deployment of forces in Eastern Europe as a deterrence against Russia, our forces are also expected to conduct a vigorous defence against disinformation and to prosecute a proactive, aggressive and truth-based information campaign that brings all our capabilities to bear.

We trust that the particular assets, mindset and nomenclature – such as "enemy," "target," "threat" and "non-munition capabilities" – that inform use on the physical battlefield remain carefully controlled and compartmentalized, and not employed on the home front in routine domestic operations and activities.[2] That is not just a reasonable expectation but a necessary condition for public trust and confidence in a national institution with real power and profound responsibilities as its raison d'être. Should this understanding be broken, the CAF's ability to operate effectively at home and on missions overseas would be severely impaired.

This is because organizational reputation and institutional credibility are existential conditions for Defence and have valuation like bankable assets. When tasks such as support to long-term care facilities or help to First Nations communities fighting a pandemic go well, the good will account balance increases. When the DND/CAF do poorly, such as their long-standing challenges of managing major procurements, or dealing with military sexual misconduct and inappropriate behaviour, the account is drawn down. Too many withdrawals from the available reserve have real consequences that impact recruiting, retention and the willingness of decision-makers to buy the

[1] Department of National Defence, CDS/DM Directive – Response to Reviews of Information Operations and Influence Activities, June 9, 2021, 7.

[2] There are caveats to allow invasive activities by military information-related capability assets against Canadians, in Canada. Examples include actions by military counter-intelligence to identify, monitor and act against far-right activists in the CAF; the Communications Security Establishment (CSE) providing cyber-support to an agency that requests assistance, like the RCMP; or the use of electronic warfare during a counter-terrorism operation. These are exceptional circumstances of use conducted under carefully controlled conditions with strict authorities, with the activities subject to independent external oversight.

military's preferred choices of multi-billion dollar equipment.[3] This trust balance also directly impacts public willingness to support military operations outside Canada, especially those that could or do result in deaths and casualties.

Public trust in Defence is a national security imperative. As the adage says: "Trust is gained by the teaspoonful, and lost by the bucketful." The CAF has been in the latter very uncomfortable space before (Somalia), when actions, decisions and public communications were not aligned with Canadian values. At the time, many serving members wondered how, or even if, the institution could survive and recover. Independent external expert advice and top-down political direction were needed to compel important reforms that the DND/CAF was unable or unwilling to do of its own volition.

The CAF is now struggling to extract itself again from a deeply hurtful crisis of its own making.[4] As Minister of National Defence Anita Anand said on behalf of the government in her apology to victims, the "misconduct and abuse of power led to a crisis of broken trust in the Defence Team."[5] Some senior military leaders and national politicians attribute this lamentable situation to a "military culture that needs to change," especially as it relates to inappropriate and negative behaviour, including systemic harassment, discrimination, racism, misogyny, hateful conduct, abuses of power, systemic barriers, unsupportive environments, lack of inclusion, micro-aggressions, bullying, intimidation, threats, violence, employment inequity, unconscious biases and sexual misconduct. These behaviours described by Defence are "rooted in an institutional culture," that prevented the CAF "from evolving apace with the rest of society."[6] An independent review led by former Supreme Court Justice Louise Arbour is seeking answers as to how this came to be. We should not expect that inappropriate behaviour toward other members inside Defence is the only abject consequence of this military-society disconnect.

In fact, we can confidently observe evidence this insidious side to military culture is manifest elsewhere, and publicly acknowledged by the DND/CAF's senior leaders. The summary is as follows: A five-and-a-half-year-long effort at National Defence – referred to in this paper as the Military Strategic Communications (MilStratCom) initiative – called into question the DND/CAF's commitment to truthful, objective and appropriate public communication at a time

[3] For instance, the spring 2012 Auditor-General's "Replacing Canada's Fighter Jets" report exposed the effort by National Defence to downplay project risk, skew mandatory requirements and fudge cost figures to secure cabinet approval for the jet it desperately wanted through a sole-source purchase. This influence scheme affected government and central agency (Finance, Treasury Board, Privy Council Office) confidence in the DND/CAF, leading to major delays and increased costs to replace the jets and ancillary platforms such as air-to-air refuelling aircraft. It also led to serious delays on other major procurements increasing those costs and DND lost its spending authority for routine purchases for years, though this has since been restored. Ten years later, the DND/CAF are just now learning which platform is proposed to replace the CF-18.
[4] Chief of the Defence Staff Wayne Eyre and other senior military leaders have frequently characterized the military sexual misconduct/cultural change issue as being an "existential" issue and/or crisis. See https://www.canada.ca/en/department-national-defence/news/2021/11/speech-by-acting-chief-of-the-defence-staff-general-wayne-eyre-at-the-kingston-conference-on-international-security.html. Accessed January 22, 2022.
[5] See https://www.canada.ca/en/department-national-defence/news/2021/12/dndcaf-sexual-misconduct-apology--minister-of-national-defences-apology.html. Accessed January 10, 2022.
[6] Department of National Defence, CDS/DM Initiating Directive for Professional Conduct and Culture, April 29, 2021. See: https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/04/initiating-directive-professional-conduct-culture-cds-dm.html and https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/chief-professional-conduct-culture.html. Accessed January 10, 2022; and National Defence, "Conduct and Culture Change Progress Tracker." Accessed March 15, 2022.

when truth decay, misinformation and disinformation have gained much traction around the world, including in Canada.

The initiative began in mid-2015 and was shuttered in November 2020, at least in the form it took at the time. This was part of a broad effort to make Defence more effective abroad and at home by evolving how it organized, co-ordinated and conducted its communications, actions and activities to influence target audiences' attitudes, beliefs and behaviours. In so doing, initiative leads and institutional leadership, inadvertently or otherwise, set conditions to use information operations (IO), psychological operations (PSYOPS), influence activities (IA) and military deception against Canadians and allies.

The haphazard manner in which the effort was organized, managed and governed meant that policies, lexicon and activities established conditions for unapproved adventurism by members enjoying unrestrained initiative in the informational space. This also led to online attacks by senior Public Affairs officers (PAOs), tacitly sanctioned by senior leadership, against media and others critical of Defence to try to influence coverage. Considerable negative news stories accumulated (see Appendix 2). Had the project become fully operational, without having policy making clear the distinct boundaries between activities allowed overseas and in Canada, succinct approval processes, and appropriate governance and oversight, significant long-term reputational damage was a certainty. The initiative would have damaged the Defence program for many years, affected the conduct of military operations and core DND/CAF functions and harmed national security.

Events revealed significant areas of concern related to culture in certain quarters of Defence that should be of keen interest to military and political leaders, if not formal inquiry. This includes a contemptuous attitude by some operator communities to oversight, direction and guidance by superior HQs; a general disdain for civilian authority and civilian advice; an allergy to external agents and oversight; a fundamental misunderstanding of the media's role in society; and the failure of DND/CAF leadership to ensure effective management of a defence policy initiative central to operations, reputation and credibility. This was DND/CAF leadership's wilful negligence, military practitioner hubris and communications malpractice.

By the end of Gen. Jonathan Vance's tenure as chief of the defence staff (CDS) in mid-January 2021, four internal investigations into missteps by different elements of the communications function during 2020 alone were in the hands of senior leaders. In June 2021, then-acting CDS Lt.-Gen. Wayne Eyre and then-deputy minister Jody Thomas assessed in writing that "sometimes insular mindsets" had eroded public confidence in the CAF, unapproved policies were "mistaken as authoritative," and that senior-level direction and guidance had been lacking, the result being ineffective oversight of the MilStratCom initiative. They also characterized the overall effort and the associated plan as being "…incompatible with [government of Canada] Communications Policy and DND/CAF vision, mission and principles of Public Affairs."[7] Direction has been given

[7] CDS/DM Directive – Response to Reviews of Information Operations and Influence Activities, June 9, 2021.

to reset the effort. At issue is whether measures to date are sufficient to avoid a repeat of the events soon to be described: this paper will explain why leaders should still be concerned and why a status quo approach is dangerous to Defence and to our national security interests.

In Canada? How is this even possible? What happened? The subject is rich with lessons observed (lessons are not learned until the condition noted has been accepted and actions change). The default response of large institutions like National Defence to unsatisfactory outcomes is to "look ahead, not in the mirror" and press on, the fix inevitably being more resources and more training. This time, though, the DND/CAF need a careful assessment of the underlying reasons to help inform a viable way forward for decision-makers and practitioners. This monograph is such an effort, seeking to understand the origin of events and how identifiable patterns and knowable problems were allowed to grow out of control. The rise and fall of the MilStratCom initiative in Canada illustrates many of the challenges that all militaries face trying to navigate through the informational space, and thus has real applications for other NATO members and partners.

The story is complicated and unpacking it takes time, partly a function of the chore it is to navigate through terminology the military uses to explain the subject to itself. Many of the terms in use such as influence campaigns, information operations, deception and psychological operations are now quite commonplace in public discourse for nefarious reasons and historical association, even if they don't mean the same to military practitioners. Also, events transpired over a long time in a non-linear fashion, with policy evolving in fits and starts along multiple, overlapping lines of disconnected effort.

This monograph consists of eight sections, chapter I being this introduction. Chapter II explains the rationale and impetus for the MilStratCom initiative, operator and practitioner perspectives of the problem, overall aims, relevant lexicon and the appeal to certain groups in the CAF. Chapter III explores key documents that informed decisions and actions illustrating the underlying intent and philosophy of the effort, setting conditions for the exercise of poor judgment and misapplications of policy in practice.

Chapter IV explains how the initiative came unglued in 2020, describing six incidents that were the subject of embarrassing media coverage and exposed weaknesses in the strategy to that point. Chapter V sets out the findings of the various internal reviews commissioned following missteps in 2020, and how senior leaders tried to right the ship. Chapters VI and VII reflect on 10 lessons observed and offer 20 recommendations for senior leaders' consideration to recover from the setback and take necessary work forward. Chapter VIII concludes by summarizing the tale and findings. Readers may find the timeline (Appendix 1) and condensed version of events to be a useful signpost to help make sense of the evolution of key developments and their meaning. Tables 1 and 2 offer more concise summaries of two different topics: contrasting the myths and misconceptions of the MilStratCom initiative operating philosophy with the reality; and setting out the main thematic elements of the approach taken, compared with how it might otherwise have been organized to better effect (and should still be).

II: A Wicked Problem Set

The Information Environment – Overview

We are awash in a daily tsunami of misinformation, malinformation, disinformation and fake news, which is upending long-held norms of (relatively) reasonable public discourse.[8] This is tearing at our social fabric, politics, economy, physical security and mental wellbeing, and bears directly on our national security. No country is immune to these forces. Feelings of disconnectedness and powerlessness are accelerating and manifest themselves in many ways: in the U.K. it was Brexit; and in the U.S., the 2016 and 2020 presidential elections, including a seditious conspiracy. There is also the response to the COVID-19 pandemic, which some still consider a hoax, but is on track to kill one million Americans by May 2022.[9] Canada, normally sedentary by comparison, has been beset with protesters blocking access to hospitals administering life-saving vaccines, various trucker "freedom convoys," including a siege in the nation's capital, and recently, high-profile incidents of far-right, anti-government activity by members of the Canadian army.[10]

The loss of citizen faith, trust and confidence in government and political leadership may be the fundamental threat of our times for liberal democratic societies – arresting that trend and then restoring trust is the ultimate challenge. How successful our leaders and institutions will be at that will require meaningful progress on longstanding issues of systemic economic and social inequities and feelings of disenfranchisement, while concurrently tackling global challenges including climate change, sustainable energy, security, and an ongoing pandemic.

---

[8] The distinctions are not always tidy but a generally accepted taxonomy is a necessary first step to understanding, then tackling the issue. Disinformation is deliberately created false or manipulated information to mislead and deceive with the express intent to obtain political, personal or financial gain; it is often associated with state-sponsored activity but is not limited to that. Malinformation is deliberately manufactured content about a person, organization or country, with at least some truth, but with seriously twisted context. Misinformation is the unintentional sharing of content that is wrong or creating content that is unknowingly incorrect.
While not a new term, "fake news" achieved widespread notoriety as a favourite expression of former president Donald Trump to criticize stories and sources he did not agree with. Fake news is generally understood to be fabricated information that is obviously wrong and is a subset of disinformation. It also refers to false stories that appear to be news, including satire like the Babylon Bee ("Fake News You Can Trust"), the Onion ("America's Finest News Source") or the Duffel Blog, writing about the U.S. military and veterans. Some of this content is cleverly done and stories have frequently been cited and shared by outraged politicians and commentators on social media, believing them to be true: thus, fake news that is disinformation that when believing to be true is shared, becomes misinformation.
The challenge, of course, is that what constitutes fake news is in the eye of the beholder, often being a subjective opinion and ideologically based. For instance, for the millions of Americans who legitimately believe the 2020 U.S. presidential election was stolen, Fox News is a reasonable and reliable news source about this subject and CNN a purveyor of malinformation and disinformation. There are now many valuble valuable resources exploring these concepts and phenomena. Three of particular note are Claire valuable resources exploring these concepts and phenomena. Of particular note are: Wardle and Hossein Derakhshan, "Information Disorder Report," Council of Europe DGI(2017), 09 2017; U.K. Government Communication Service, "RESIST Counter-disinformation Toolkit," 2019; and Maria D. Molina, S. Shyam Sundar, Thai Le and Dongwon Lee, in "'Fake News' is not Simply False Information: A Concept Explication and Taxonomy of Online Content," *American Behavioural Scientist*, Oct. 14, 2019. Two valuable books on the subject are: Cindy Otis, *True or False:A CIA Analyst's Guide to Spotting Fake News* (New York: Fiewel and Friends, 2020); and Carl Miller, *The Death of the Gods: The New Global Power Grab* (London: Windmill Books, 2018).

[9] See Johns Hopkins Coronavirus Research Centre, https://coronavirus.jhu.edu/region/united-states, Accessed January 10, 2022.

[10] Patrick Matthews was sentenced to nine years in prison for his role in trying to incite a race war in the U.S.; Corey Hurren crashed the gates at Rideau Hall with his vehicle and wandered the grounds with loaded weapons, looking to "speak with" Prime Minister Justin Trudeau; and Erik Myggland was kicked out for links to far-right groups and obscene social media comments, including against national leaders.

Astounding advances in communication technology have exacerbated these fault lines. In his iconic 2007 keynote speech introducing the iPhone, Steve Jobs said: "Every once in a while, a revolutionary product comes along that changes everything."[11] Indeed. Since then, an estimated 14 billion smartphones have been sold, with nearly 92 per cent of the world's population now having a smartphone or mobile phone.[12] The internet's dramatically improved functionality and broad access to devices and wireless at an accessible price point fuelled an explosion of platforms, apps and social media providing easy access to vast amounts of content. This has dramatically altered the ecosystem of how we create, receive, process, share and use news and information.

Almost anyone in the world can generate and share content including high-quality video, anonymously if desired, at little cost with a worldwide audience in real time. This brought together heretofore discrete, disconnected communities of shared interests and passions, and changed how we live, love, play, shop, learn and work. The flip side of course is that the same technology has helped connect ne'er-do-wells, conspiracy mongers, malign actors, white supremacists, terrorists and anti-vaxxers alike to attract new recruits to their causes, and enabled them to share, validate and propagate their particular views, biases and prejudices. As Robert Bateman observed: "Once, every village had an idiot. It took the internet to bring them all together."[13] This has made it difficult for the merely misinformed or the truly curious to distinguish between fact, opinion, guess, conjecture and falsehood. Technology, but social media in particular, has made secrets harder to keep, allowing people to almost instantly compare what they hear from public sources with participants in the events.

A cut-and-dried case of victim (Ukraine) vs. aggressor (Russia), with a narrative pretence for war as outlandish as "denazifying" and "demilitarizing" the former to protect the latter, even finds traction in and outside of a media- and civil society-oppressed country like Russia. For example, in response to the question: "Is Russia committing war crimes in Ukraine?" Canadian social science researcher Frank Graves of EKOS found 88 per cent of those polled who had received at least three doses of COVID-19 vaccine agreed and three per cent disagreed. Of those who refused the vaccine, only 32 per cent agreed with the question, with 42 per cent disagreeing.[14] The data also showed a very high correlation of "disagree" with voters for Canada's far-right party. This is compelling evidence of a wicked problem: we have easier access to a wider array of information than at any time in history, but the way that tablets, phones and social media platforms combine individual tastes, interests and likes to deliver personally tailored information creates increasingly impenetrable echo chambers that confirm existing or latent biases.

Civil society has started to fight back against mis- and disinformation. Social media giants such as Facebook and Twitter are under increasing pressure from legislators, the public, their own users and even current and former employees to improve how their platforms deal with malign content. Settling on what is an acceptable threshold and moderating content is an especially

[11] See https://www.youtube.com/watch?v=x7qPAY9JqE4. Accessed January 10, 2022.
[12] Estimates of this and numerous other communications technology-related usage data available at www.statista.com.
[13] Quoted in Peter Singer and Emerson Brooking, *Like War: The Weaponization of Social Media* (Boston: Mariner Books, 2018): 126.
[14] The survey was conducted with 1,035 persons. See https://twitter.com/VoiceOfFranky/status/1504652043482542080/photo/1. Accessed March 19, 2022.

daunting challenge. Organizations like the Atlantic Council's Digital Forensics Lab, the Carnegie Institute's Partnership for Countering Influence Operations, the Check My Ads Institute (billing itself as the advertising technology's watchdog with a mission to "dismantle the disinformation economy") and, in particular the formidable research group Bellingcat, have had notable successes exposing harmful and hateful online campaigns as well as the money behind them.

Some jurisdictions have woken up to the urgency of the threat and invested in inter-agency and inter-governmental efforts to build their nations' resilience to deceptive influence practices. For instance, Finland hosts the European Centre of Excellence (CoE) for Countering Hybrid Threats; Latvia has established a NATO-affiliated CoE for Strategic Communications; and Sweden has announced it is establishing a Psychological Defence Agency, with 45 staff.[15] The Global Engagement Center, run out of the U.S. State Department, is a major player with a variety of innovative initiatives.[16] The U.K. has made significant inroads by detailing a bold national strategy and program for online media literacy, information-related capability investments in the U.K. military and a best-in-practice Government Communications Service (GCS). Canada is late to the game. While beginning to make some modest investments and hinting at regulation of social media platforms operating in the virtual battleground, the federal government lacks any overarching strategy or obvious central body to generate co-ordinated momentum to do better. Experts are not unfairly decrying its efforts as "shrouded in mystery" and "a bit of a black hole of information."[17] Notably, the April 2022 federal budget proposed $10 million over five years for

[15] Emma Wollacott, "Sweden Launches Psychological Defense Agency to Counter Disinformation," *Forbes*, January 5, 2022, https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation/?sh=38d79a764874. Accessed January 10, 2022.

[16] The Center's mission is: "To direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations." See: https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/. Accessed January 10, 2022.

[17] See Anja Karadeglija, "Melanie Joly Vows to Tackle Virtual Battleground of Russian Disinformation," *National Post*, March 21, 2022, https://nationalpost.com/news/politics/melanie-joly-vows-to-tackle-virtual-battleground-of-russian-disinformation. Accessed March 21, 2022. The most notable effort at countering disinformation by the Canadian federal government came in 2019 with the announcement of a co-ordinated effort to protect the integrity of the (at the time, unknown) next federal election, in acknowledgment that "foreign and malicious actors are becoming more creative at using online platforms to manipulate opinions." This included establishing a Security and Intelligence Threats to Election (SITE) Task Force; Government of Canada, "Government of Canada Unveils Plan to Safeguard Canada's Election," January 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/government-of-canada-unveils-plan-to-safeguard-canadas-election.html. Accessed January 10, 2022. Canada through Global Affairs leads the G7 Rapid Response Mechanism, introduced at the G7 Summit in Charlevoix, Que., to deal with threats to G7 nations, including disinformation. More than $13 million has been provided and another $3 million to help Ukraine combat Russian disinformation. See https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng. Accessed March 15, 2022. The April 2022 federal budget also proposed an additional $13.4 million over five years to expand the initiative. See Department of Finance Canada, *Budget 2022*, 142.
The Communications Community office within the Privy Council Office, where one might expect to find a cross-department effort in this regard, remains a grouping of government communicators focused on personal skills development, recruitment and career networking for the practitioner community; of the 18 areas of practice accessible only on the government online network, none is dedicated to helping build societal or government information resilience. See https://www.canada.ca/en/privy-council/services/communications-community-office/about-communications-community-office.html. Accessed January 10, 2022. In March 2022, the independent Canadian Radio-television and Communications Commission (CRTC) banned Russia Today and RT France from Canadian airwaves, in view of programming that "undermines democratic institutions within Canada." See Peter Zimonjic, "CRTC bans Russian State-controlled TV Channels RT, RT France from Canadian Airwaves," CBC, March 16, 2022, https://www.cbc.ca/news/politics/crtc-russia-today-broadcasting-decision-1.6386929. Accessed March 16, 2022. In June 2021, at the NATO Summit in Brussels, Prime Minister Justin Trudeau announced Canada's intention to establish, host and be the framework nation for a new NATO Centre of Excellence (CoE) on Climate and Security; there are now 27 NATO-accredited CoEs, none in

the Privy Council Office to "coordinate, develop, and implement Government-wide measures designed to combat disinformation and protect our democracy."

Current and recent momentous events have vividly demonstrated the critical, central role of trustworthy, timely and quality government communications to our lives, and the massive challenge now of doing that well. The pandemic has exposed deep fissures of mistrust and illustrated how seriously difficult it is for governments to explain, convince, persuade and even incentivize (or coerce) populations to change fixed attitudes and behaviours, even when outcomes are serious illness or life-and-death. It has taken a monumental and unprecedented effort by governments and civil society to convince people to do their part, even if just to wear a mask and socially distance to reduce the spread of COVID-19, lower the odds of more virulent strains emerging and take pressure off hospitals and ICUs. This, despite near-continuous communications by top elected leaders for more than two years, including months-long stretches of daily news conferences featuring the most senior public health officials, non-stop media coverage, stringent health protection measures, sanctions including job loss, and multiple reminders as all have tried to go about their lives outside the home.

It remains to be seen what the loss of public trust in government will mean for the ability to govern effectively. Two takeaways of note are pertinent to this discussion. First, any chance of success for complex initiatives requires right policy, good operational execution and an excellent communications effort. This puts an absolute premium on investments in the latter – to be effective, government communications need to demonstrate real leadership-driven commitment to the function, underpinned by capability and capacity, supported by a comprehensive, co-ordinated, continuous and consistent effort and output (a "7C" model).

Second, events have demonstrated the real limits of government and civil society's ability to influence attitudes, beliefs and behaviours – and the limits of "narrative" – even at home, speaking the same language and with shared culture (if not always shared values). Many believe that a virus that has killed millions is a hoax; that Bill Gates is behind COVID-19 so tracking devices can be implanted in humans; that the 2020 U.S. election was stolen and Joe Biden is an illegitimate president; and that there is merit to ingesting bleach, using horse medicine or drinking urine rather than heeding the best advice of leading scientists and health-care practitioners. For these people, no amount of narrative, no matter how cleverly formulated, is going to shift their view.

We should not be surprised then that our military inform-influence-persuade-coerce efforts overseas in places like Afghanistan, Libya and Iraq have fallen so short. Not only are we still surprised, but the institutional reaction is to keep doing the same things the same way, as if handing out more, cleverly done PSYOPS leaflets would somehow tip the balance in our favour.

Canada. These serve to concentrate expertise in a subject and help share knowledge as well as leading research in the field and best practices. In view of the mis- and disinformation associated with climate change, it will be interesting to track the extent to which strategic communications features into the new Canadian CoE's organizational design and operations.

As one practitioner explained, "The greatest success of CAF information operations operators has been their ability to influence CAF leaders into believing that they were having a serious impact."[18]

The Problem Set – The Operator Perspective

There is broad agreement within Defence about the ends the institution desires to accomplish with reform of the communication functions:

- Set information effect more clearly at the core of operational design and planning;
- Obtain obviously better strategic communication outcomes not just better public affairs (PA);
- Develop a planning framework to synchronize overarching institutional and operational efforts including actions and key leader engagements (KLE); and
- Enable more strategic, deliberate and proactive consideration of the information space of all decision and activities within Defence. As noted Australian strategist David Kilcullen has observed, "Building a strategic information warfare capability is perhaps the most important of our many capability challenges in this new era of hybrid warfare."[19]

There are three main reasons behind the CAF's interest in information-related capability reform. First, adversaries such as Daesh, al-Qaeda and the Taliban were highly successful purveyors of influence campaigns to tell their stories and enable operational success, including recruiting more to their ranks. Mischievous states like Russia, China, Iran and others were also realizing great returns on their investments in radio, print, high quality, government-run, overtly propagandistic TV networks and offensive information warfare/influence operations. These included bot farms generating thousands of social media posts a day deliberately targeting NATO nations, including Canada, with mis- and disinformation.[20]

The second reason was acknowledgment that Defence's strategic communications challenge was considerably broader and deeper than just the public affairs function – even though that tended to attract all the attention and opprobrium in nearly every discussion, since the issue of the day was invariably something in the news, in Parliament or on social media – or was about to be. A measure of angst stemmed from DND/CAF activities not being optimally synchronized in the institution or with partners, reducing the prospective strategic value of the action and messaging.[21] Examples of this included how to derive more effect from the work of the many

[18] Exchange with Influence Activities officer practitioner, February 2022.
[19] David Kilcullen, *Accidental Guerrilla* (London: Hurst & Co., 2009): 300.
[20] See Canadian Security Intelligence Service, "Foreign Interference: Threats to Canada's Democratic Process," July 2021; and Monika Gill, Ben Heap and Pia Hansen, "Strategic Communications Hybrid Threats Toolkit," (NATO Strategic Communications Centre of Excellence, September 2021).
[21] All decisions and actions or inactions communicate something to someone, somewhere. The number of conceivable actions to influence and obtain a desired military effect are limitless and these can be tactical, operational or strategic. Should troops wear sunglasses and hand-carry or

military attaches posted around the world, or how to better leverage key leader engagements by senior CAF leaders. A planning concept or framework was necessary to provide more coherence for all the various efforts and activities.

Third, the senior combat arms/operator community widely believed that Defence PA was not fit for purpose for so-called grey-zone activities below the threshold of armed conflict. Military practitioners in the PA function were thought to be tactically proficient but strategically weak and not operational enough in terms of speed, agility, focus, advice, content produced and outcomes. Commanders were increasingly frustrated at not getting the results they wanted – the adversary's behaviours are not changing! – and the ubiquity of 24/7 public affairs in the information environment was an easy scapegoat for every problem of insufficient policy, shortcomings of execution or mediocre leadership. Too many senior officers also held the ADM PA Group in palpable contempt, having long considered them to be unduly focused on ministerial/deputy minister/DND institutional communications compared to CAF military communications.[22]

The Problem Set – The Practitioner Perspective

The two main information-related capability DND/CAF practitioner communities working in the cognitive space (how people think and act) fall roughly into two camps: the IO/PSYOPS fields that do influence-and-coerce abroad, and military and civilian PA doing inform-and-persuade at home and abroad.[23] Canadian practitioners have published very little about what the IO function does and how it performs on operations. The one notable example comes from an IO officer formerly with the Canadian-led battle group operating in Latvia as part of the NATO deterrence mission. The deployment borders Russia and thus is a highly contested information space. Major Chris Wattie notes the IO team was able to respond to basic nuisance allegations, such as news reports

sling weapons (or not bring them) when meeting local leaders in Afghanistan? To maximize key DND/CAF leader engagements and avoid sending mixed messages, which senior military leaders need to visit which counterparts, when and where, to discuss what and to offer/ask for what?

Many actions have strategic effect. For instance, sailing a HMCS ship through the Taiwan Strait or near the disputed Spratly Islands in the South China Sea to demonstrate freedom of the seas and international right of passage, sends a message to China and one that appeals to many in Defence. That same action though, may serve to increase tensions with that country at a time of delicate Global Affairs-led Canadian hostage negotiations. A decision to embed a Canadian reporter on board ship to publicly document such a trip, including with imagery, can dramatically amplify an otherwise quiet message. Dispatching the ship (or not) as part of a fleet with coalition or NATO partners also sends a different strategic message. These and many other decisions are informed by, but not just by, military considerations. There are also actions that communicate at the grand strategic level, such as the decision for Canada to lead a NATO battle group stationed in Latvia as a deterrence to Russia and to reassure the Baltic states. And the government's decision to proceed with negotiations with Lockheed Martin (U.S.) to purchase the F-35 joint strike fighter over the Saab JAS 39 Gripen (Sweden) will send a decisive message lasting decades, to Canada's most important ally.

[22] The deputy minister (DM) by level is equivalent to the CDS in rank, and by Treasury Board policy has important accountabilities and responsibilities for the DND communications function. The functional authority, or head of communications, is the assistant deputy minister (Public Affairs) or the ADM (PA), a civilian three-star equivalent. At the best of times, there are differences of opinion about the breadth and scope of the DM's remit in what some uniformed personnel consider CAF business and the exclusive purview of the CDS. During periods of intense activity or turmoil such as that experienced by National Defence in 2021, these pressures are exacerbated and who is seen to be involved in what issue between CDS and DM both internally and in public communications causes frictions. See former Defence DM Jody Thomas's comments in Canadian Global Affairs Institute, Battle Rhythm podcast episode 49, "Healthy Tensions," May 19, 2021, https://www.cgai.ca/healthy_tensions. Accessed January 10, 2022.

[23] This is a general description for ease of explanation. The imagery technician trade is arguably a distinct group but Public Affairs is the functional authority for it.

of the contingent employing a barber from Canada rather than someone local, or the Russian narrative suggesting the NATO soldiers were a potential source of COVID-19 infection. His take, though, is a devastating indictment of the CAF IO capacity and capability to support deployed operations. [24]

The MilStratCom Public Affairs community assessed five main deficiencies with the PA function: insufficient military culture, expertise and readiness; reactive, rather than strategic-driven engagement; ineffectual management of visual communications; lack of innovation; and insufficient CAF capacity and mindsets. The conclusion: this "results in ineffectual engagement in the military information domain and global information environment."[25] The description – while not entirely undeserved – was a one-sided interpretation of a complex suite of factors that militated against doing better. The characterization also served to encourage, not disavow, leaders and operators of their perceptions about PA, and gave them yet another pass for the situation being the way it was.

The diagnosis was not confined to military practitioners. A notable feature of the culture at work was how common it was for some military PAOs to unkindly judge civilian communication colleagues because of their different terms of service. Uniformed members served with unlimited liability and quite likely, at some points of their career, while on operations, provided advice about decisions of considerable consequence including to targeting boards to determine and eliminate operational targets. As the MilStratCom PAO lead described it, while there were advantages to civilian-led Public Affairs, it had led to "a lack of focus on martial imperatives," leading some practitioners to become "corporate PR agents" more focused on "recruiting and other benign institutional priorities," when the need was for "information warriors."[26] There are in fact notable distinctions regarding a military practitioner's type of service compared to their civilian counterpart, but the effort to favour the former over latter created unhelpful friction.

What's In a Name: The Tyranny of Terminology

The careless application of some key terms during the MilStratCom initiative factors considerably in this story. Understanding why is important to help inform a way ahead and avoid a repeat of the outcome. The terminology the CAF used in related doctrine, policy, staff work and the conduct

[24] Wattie's assessment is highly critical at least of the 2019-2020 period in question. His experience: the CAF does not have the means to identify information attacks, their source or their potential impact; support "from higher headquarters in Canada has been limited at best" – a reference to Canadian Joint Operations Command (CJOC) and the Strategic Joint Staff which is the functional authority for IO; assessment of effects is "simply not a priority for staff in the Task Force;" there was "no bank of approved messaging or themes issued by higher authority;" only four of the nine military staff in the group had information activities training; and there was no dedicated budget or vehicles, or even translators or cultural advisors attached to the cell. Most damningly, "currently, task force planning and activities are focused almost exclusively on the conventional, kinetic capabilities … the mission is seen in terms of deterring and if necessary defending Latvia against a conventional Russian attack." See Maj. Chris Wattie, "Bringing a Knife to a Gunfight: Canadian Strategic Communications and Information Operations in Latvia, Operation Reassurance 2019-2020," *Canadian Military Journal*, vol. 21, no. 1, Winter 2020.

[25] Canadian Armed Forces/ADM(PA) Military Strategic Communications Group, Military Public Affairs Enhancement and Employment Concept (MPAEEC), (version 9.2, October 2020), 8-9. (See ATIP A0527354).

[26] Various, including Canadian Armed Forces, Military Strategic Communication and Public Affairs Operationalisation Force Development Plan (drafts April 26, 2019 and June 7, 2019, 11. (See ATIP 0527355).

of operations is rife with multiple meanings – *information* operations, *strategic* communications, *psychological* operations, *influence* activities. Language like "non-munitions-based capabilities" and "targeting" jars sensibilities when used in a domestic context. As the CDS and DM noted in guidance issued in November 2020 – but after the MilStratCom initiative had been terminated – "the loose or incorrect use of many of the terms associated with information-related capabilities … create considerable confusion of intent within DND/CAF and in particular with outside audiences."[27]

Information Operations (IO)

In the public consciousness, IO is frequently equated with high-profile campaigns by slick operatives using nefarious data and social media manipulation techniques to affect perceptions and realize significant objectives at home. These objectives include Brexit, the 2016 and 2020 U.S. presidential elections, and galvanizing support, at least initially, for the "freedom" trucker convoys in Canada. The term is also regularly applied to international state-sponsored activities such as when Russia disguised who shot down Malaysia Airlines Flight 17 over Ukraine; as an instrument by Russia to provide a cover for the annexation of Crimea in 2014;[28] and to establish the pretence to again invade Ukraine in February 2022. To non-military audiences, IO has the same negative connotation as "psychological operations." Facebook, the social media giant trying to find ways to combat misinformation on its platform, defines IO as "coordinated efforts to manipulate or corrupt public debate for a strategic goal."[29]

The term has a different meaning in the military, but even so, remains widely misunderstood inside National Defence. First and foremost, IO is a staff function that seeks to plan and co-ordinate the efforts and actions of a wide variety of military capabilities and assets; the responsible IO staff do not actually do anything with the information, such as creating content for publications (this is the work of groups like PSYOPS or PA), or jamming an adversary's communication network (this is the work of electronic warfare units).[30] Confusion arises in part because IO refers to the people who do the activity, the work processes and also the associated capabilities.

Information operations take place in the information environment, defined as "the information itself, the individuals, organisations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs" – meaning how everyone thinks and acts, plus the processes for managing and using information including data and the physical

[27] Department of National Defence, CDS/DM Planning Guidance: Enhancing Operational and Institutional Communications: Resetting Information-Related Capability Initiatives, Nov. 12, 2020, 6.
[28] Alan Kelly and Christopher Paul, "Decoding Crimea: Pinpointing the Influence Strategies of Modern Information Warfare," NATO Strategic Communications Centre of Excellence, 2020.
[29] Facebook, "Threat Report: The State of Influence Operations 2017-2020," May 2021, 3, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf. Accessed January 10, 2022.
[30] In CAF policy, the capabilities and functions associated with IO are set out as: civil-military co-operation (CIMIC); cyber-operations; electronic warfare; engagement; deception; operations security; physical attack; special technical operations [op secret, black arts activities]; presence, posture and profile; PSYOPS and Public Affairs. This is not an exhaustive list. All actions communicate something to somebody somewhere, and so actions are a part of IO. From Department of National Defence/Canadian Armed Forces Policy on Joint Information Operations (April 2018, 3). (See ATIP A0509895).

assets.[31] In Canada and NATO, IO are "coordinated actions to create desired effects on the will, understanding and capability of individuals and groups … by affecting their information, information-based processes and systems while exploiting and protecting one's own": as such, IO has offensive and defensive features. The aim of IO actions is to "induce, reinforce, convince, encourage, or even coerce" the approved target by affecting behaviours, perceptions, attitudes and their will. An infinite number of actions or engagements can be had – per Canadian IO policy, these being, "any form of human interaction aimed at communicating messages in support of the overall campaign objectives."

Information is ubiquitous: it is a part of the physical world (things), the virtual (information itself) and the cognitive (how people think and react). The military essentially has defined IO *as everything*, including the actual effort of trying to subject everything to a process based on information co-ordination meetings and working groups.[32] Of course, it is quite impossible to predict and co-ordinate everything related to information in just the right way to obtain a desired military outcome.

IO has three distinct facets. First is a technical application to acquire information and data to assist with targeting, or to protect our systems from being compromised by an adversary (relating mainly to cyber, space and electronic warfare functions). Second are actions that are overtly coercive involving bombs, missiles, bullets and other munitions, the deployment of forces, the threat of same or deceiving an adversary into revealing their position or capabilities (thus relating to the functions of physical attack and military deception). Third are inform-influence-persuade activities that pretty much any element of the military can undertake. On deployed operations overseas, this is most often associated with Public Affairs activities, PSYOPS products like leaflets and "presence" activities such as troops interacting with local populations, including community engagements and *shuras*.[33]

The IO model does not distinguish between scale or impact. Deploying an aircraft carrier loaded with advanced weaponry to the Gulf region; sending a 120-person artillery unit to Latvia or putting 3,400 soldiers on notice to deploy to Eastern Europe; using a tactical nuclear weapon to destroy a target; or issuing guidance to use the word "enlargement" rather than "expansion" in public communications about NATO are just tools and actions intentionally designed to influence an adversary or audience. By longstanding policy, doctrine and practice, IO activities are well understood to be subject to strict authorities and restricted to use on deployed expeditionary

[31] NATO, Military Committee Policy on NATO Information Operations 422/5, January 22, 2015. This is also the definition in the Canadian Joint IO Policy, 2.
[32] To obtain the skills to try to co-ordinate everything including actions, IO staff are officers or select non-commissioned officers from any trade, though in Canada that is heavily weighted to the army (RCN and RCAF do not have IO), and very often drawn from the artillery – the logic being those who wear that cap badge are grounded in the process of acquiring and engaging targets. Those with a qualification in IO will most likely have taken the IO Officer course in Canada (10 days), or the U.K. (10 days), or NATO (10 days): the U.S. course (12 weeks) qualifies the student in IO and military deception (Mil Dec) and can be a career specialization. The Canadian course is in the process of being made significantly longer.
[33] The number of actual and possible inform-influence-persuade military activities is endless. Some actual examples: a radio station run by Canadian PSYOPS broadcasting content to Kandahar province to convince Afghan poppy farmers to switch to licit crops; PA holding a news conference to persuade recalcitrant Bosnian Serbs to allow NATO forces to inspect weapons cantonment sites and turn over persons indicted for war crimes (PIFWCs) and (informing?) them if they don't comply within a day, they would be subject to armed attack; and CAF units deployed to Latvia, hosting hockey games as a bit of community outreach or conducting live-fire exercises with other soldiers from NATO.

operations such as in Afghanistan against the Taliban, coalition operations in the Middle East against Daesh or with NATO forces deployed in Latvia to counter Russian disinformation – not on operations in Canada. This understanding changed during the MilStratCom initiative, which sought to expand IO activities domestically.

As if that were not confusing enough, into the mix came strategic communications (StratCom), another process integrator and staff function that – like IO – evoked similar questions and wide disagreement about what it is, what it does and/or produces and at what level it is performed.[34] StratCom is yet another term widely used in business and marketing, with a very different meaning than in NATO militaries.[35] In Canada, the definition has proven difficult to nail down. The responsible Defence body agreed to the following, with MilStratCom in ADM(PA) promoting the formulation: "advancing national interests by using Defence activities as a means of communication to influence the attitudes, beliefs and behaviours of audiences."[36]

The use of the word "influence" has proven divisive, since it suggests the explicit intent of all activities, communication or otherwise, no matter how routine or with whom (such as the public or parliamentarians), is to deliberately sway a position. Even a casual reader of the terminology would find the definition remarkably similar to IO. This is because all the inform-influence-persuade-coerce tools, including actions in the IO toolkit, equally apply to MilStratCom.[37]

The difference, at least in theory, comes down to distinctions of application and where the effort is managed – IO is meant to support deployed forces on expeditionary operations, either contested or in less-than actual conflict. These activities are conducted and co-ordinated by an

[34] Conceptually, within NATO, StratCom first takes shape and form in July 2007, with publication by the North Atlantic Council of the Action Plan on NATO's Strategic Communications. This was a time of real concern about the direction of the Afghanistan campaign and realization of the urgent need to improve communication by NATO HQ about the mission and within the Afghan government. The initiatives were all about better public affairs – so, communicating with better strategic effect. In September 2009 (a week after Gen. Stanley McChrystal's explosive assessment about the situation in Afghanistan leaked to the press), NATO HQ produced the NATO Strategic Communications Policy, still extant today. In this, StratCom is described as the co-ordinated and appropriate use of five things – public diplomacy, public affairs, military public affairs, IO and PSYOPS. By NATO policy, StratCom is a political-military construct. This served the immediate purpose of being seen to be doing something on the policy front at the time, but the document is more a statement of responsibilities than an expression of desired specific effect or explicit practical guidance. In August 2017, this shortcoming was clarified with the publication of a NATO military policy on StratCom, that specifically includes military communication capabilities and military actions to inform, persuade or influence audiences.
See "The Evolution of NATO Strategic Communications," in Brett Boudreau, *We Have Met the Enemy and He is Us: An Analysis of NATO Strategic Communications: The International Security Assistance Force (ISAF) in Afghanistan, 2003-2014*. (NATO Strategic Communications Centre of Excellence, 2016), 298-348.

[35] Qualifying the type of communication as strategic suggests there are also operational and tactical forms. This is indeed the case and part of the reason for confusion since tactical activities can have strategic consequences. One such example is the U.S. IO/PSYOPS effort in September 2017 of distributing leaflets in Parwan province in Afghanistan showing a lion (representing brave Afghan forces) chasing a dog (an animal considered unclean in Islam, meant to represent the cowardly Taliban forces), with the Shahada, a profession of the Muslim faith, on the dog. This culturally insensitive activity led to local demonstrations, a suicide bomber attack injuring several people and widespread condemnation of the mission.
See Reuters and James Wilkinson,"US Forces in Afghanistan Apologize for 'Offensive Leaflet'…" *Daily Mail*, Sept. 26, 2017,https://www.dailymail.co.uk/news/article-4858004/U-S-forces-apologise-highly-offensive-Afghan-propaganda-leaflet.html. Accessed January 20, 2022.

[36] Military Public Affairs Enhancement and Employment Concept, 7.

[37] The MC 0628 NATO Military Policy on Strategic Communications is careful to insist that in order to protect public reputation, Public Affairs does not have a role in planning or conducting PSYOPS, IO or deception, though the co-ordination of activities to avoid unknowingly working at cross-purposes remains necessary.

operational headquarters like the NATO battle groups on the enhanced presence missions in Eastern Europe, or the NATO Resolute Support Mission HQ in Kabul.[38] In contrast, MilStratCom in the proposed unique Canadian concept sat above IO with applications during peace, war and conflict abroad as well as domestic applications, managed and conducted in the Public Affairs group at National Defence headquarters. In reality, there was no substantive difference in policies being proposed and practice – MilStratCom was IO by another name and meant to be used domestically.

From DND/CAF's perspective, this all leads to an unofficial hierarchy of inform-influence-persuade-coerce information-related capabilities.

Strategic Communications (StratCom): What leaders say, do and signal by their actions and decisions at the national political level. Ideally, this is a deliberate process in which the desired outcome is clearly established, which then helps inform and guide planned activities. For instance, actions to try to convince Russia not to invade Ukraine again, then to cease its attack, took many forms including diplomatic measures (recalling diplomatic officials, expulsion of Russian officials); information activities (various cabinet, bilateral and NATO meetings with various declarations and warnings); military actions (the provision of lethal aid, plus the deployment of additional NATO forces to the region); and unprecedented economic sanctions. In armed conflict though, this terminology seems quite insufficient – "political warfare" perhaps being a more apt characterization.

Defence Strategic Communications (DefStratCom): What leaders in the DND/CAF say, do and signal by their actions and decisions. This includes DND/institutional and CAF/military components.

Military Strategic Communications (MilStratCom): What leaders in the CAF say, do and signal by their actions and decisions. This implies just CAF/military actions and thus with a focus on expeditionary/deployed overseas operations, contested or otherwise, working closely with other information-related capabilities like IO, PSYOPS and deception.

Defence Public Affairs (PA): The approximately 950 civilian and military personnel who are subject to the functional authority of ADM(PA), consisting mainly of civilians in the Information Services (IS) category, plus military PAOs, and support staff.

Military Public Affairs (MilPA): Uniformed personnel doing public affairs, generally PAOs, but also including those from the imagery technician trade, such as combat camera.

[38] The problem set is inherently wicked because IO also consists of defensive activities to protect our information and information systems, which by definition have domestic applications and the distinctions that once could be made between external and domestic threats are less clear in the internet age. Some proponents argue that all operations are in fact information operations, and so IO should sit above StratCom.

Influence Activities (IA)[39]*:* A construct unique to the CAF and specific to the Canadian army, consisting of civil-military co-operation (CIMIC), IO and PSYOPS personnel.

Information Operations (IO): A staff function to co-ordinate information-related capabilities on overseas operations. In the CAF, this features in the army and special forces with an effort to expand in that space by the Canadian Joint Operations Command (CJOC).

Psychological Operations (PSYOPS): A capability to influence audiences on overseas operations. In the CAF, this is particular to the army and special forces (but not the RCAF or RCN).

The PAOs' selection of MilStratCom as the lexicon of choice for the initiative had significant impacts on events to come. By early January 2018, the term had replaced "Public Affairs" in the two senior military positions in ADM(PA) and this shaped key policy and force development work for the overall initiative. The titles of director, MilStratCom (a colonel PAO) and director general, MilStratCom (a brigadier-general PAO) were used as an influence activity to create a certain perception and desired strategic effect inside and outside Defence. CJOC followed suit with a chief MilStratCom position (a lieutenant-colonel PAO).[40]

The thinking was that this would be well received by external actors, particularly at NATO, as a sign that Canada was leading reform and change including, but not just of, Public Affairs. It also signalled that the focus of effort, energy and resources of senior military PA staff would now be directed to CAF overseas operations, not on DND or CAF institutional activities domestically. However, the new titles did not come with any explicit authority to direct and guide the associated StratCom capabilities or grant any additional access to information to better inform leader decisions or synchronize Defence actions. This was a branding effort, a useful technique to suggest to senior leaders a new approach was being tried, but without the challenge and burden of actual responsibility or any accountability for actions, missteps or outcomes.[41] The decision to name the

[39] During the pandemic response, the roles of each were explained in a briefing note to senior CAF leaders from the Joint Task Force Central HQ in Toronto. In Canadian army doctrine, influence activity (IA) refers to civil-military co-operation (CIMIC), psychological operations (PSYOPS) and information operations (IO). This is a construct unique in NATO militaries and is an army-only capability in Canada. The role of CIMIC, the note explained, "is to enable the [commander] to understand and engage the civilian component of the battlespace." The role of PSYOPS is to "weaken the will of the enemy; gain the support of the uncommitted … dominate the information environment in the [area of operations]; and countering enemy propaganda efforts." During the support to long-term care facilities in Ontario, the PSYOPS component of the influence activity team was used to create, collate and distribute print, video, imagery and social media products in English, French and Mandarin, about hand-washing and the proper use of masks, in support of Public Affairs and other government departments. From National Defence, Briefing Note for Commander CJOC, JTFC OP LASER Influence Activities and Open-Source Intelligence Production, July 8, 2020. (See ATIP A0434286).

[40] By mid-2020, leaders had developed an allergy to the StratCom and MilStratCom terms. Imagery support to exercises and select military activities such as the Nijmegen march for Public Affairs' purposes had notably improved. But the new phraseology did not have any obvious impact on the institution's ability to do any better on operations abroad or to benefit media coverage at home on the key issues of the day that needed strategic support, such as the dedication of the Afghan cenotaph at Defence headquarters, NORAD modernization, culture change or major equipment acquisition. In an effort in part to disassociate PA from the public missteps happening within the IO and PSYOPS communities, senior PA staff changed their titles and that of the initiative from MilStratCom to Military Public Affairs (MilPA). This in turn led to further confusion inside Defence, since military PA clearly distinguished CAF from DND communications. This was a name change on paper only though, and MilStratCom continued to be used for several months on personal LinkedIn accounts and in advertisements for speaking engagements outside the CAF.

[41] This all made for the very odd situation of a director MilStratCom (a PAO doing PA not MilStratCom) within ADM(PA) but not reporting to the director general MilStratCom (the senior PAO in the CAF, doing military PA not MilStratCom) and who remained infrequently involved in

effort MilStratCom and promote that, including with position titles within a unit/organizational grouping led by PAOs in the Public Affairs organization, ranks as a leading reason for the initiative's eventual failure.

Upending Policy and Practice

Vance's verbal direction to the MilStratCom lead was that any plan to re-structure information-related capabilities needed to preserve the longstanding, well-known firewall between "inform" Public Affairs and "overt influence" IO/PSYOPS and deception activities. In policy and practice, this meant two things: PA would always conduct only truthful communication and retain direct access to the commander without having to work for and report to someone with responsibility to conduct IO, PSYOPS or deception on active operations. This one degree of separation gave media and the public some assurance that the organization through its Public Affairs capability would not knowingly lie, thereby protecting institutional credibility.

Acknowledging that "integrating a MilStratCom capability in the CAF may challenge the boundaries of current national policies,"[42] the team sought ways to create "visible and identifiable" separation between PAOs doing traditional PA, and PAOs engaged in influence activities in the MilStratCom group, including IO, PSYOPS and deception.

The conundrum was to find a way to distinguish between three types of Public Affairs staff: military PAOs doing routine PA activities (for instance, Capt. Smith working in Ottawa to produce content to explain to the public the rationale and need for NORAD modernization); military PAOs in the MilStratCom group doing routine PA activities (Capt. Jones in Riga, producing content to explain the Canadian contribution to a NATO exercise in Latvia): and military PAOs with the MilStratCom group working alongside and supporting IO, PSYOPS and deception. An activity of this sort (for example purposes only), would be Capt. Williams preparing social media posts under a false name to concoct stories, or to amplify existing unconfirmed media reports that Russian senior officers in Ukraine were being killed by their own men and were committing suicide, thereby fostering the influence effect of a demoralized Russian military.

The intellectual, policy and reporting relationship contortions needed to do this were formidable and strained credulity. Three options for how MilStratCom might tackle this problem for people in that group were studied and assessed against three criteria, including the impact on the CAF's credibility, the cost and whether the change would improve operational effectiveness. The idea

actual day-to-day PA activities and planning. Within CJOC, this also meant a chief StratCom (a PAO doing PA not StratCom) reporting to a chief joint effects colonel with no related experience, three levels removed from advising the commander. This situation made it difficult to know who was responsible for doing what, made worse when the MilStratCom team in ADM(PA) extracted from DND/CAF support to work on the project full time, popping back into the daily routine where opportunity presented, to experiment and test concepts and products. This approach drew significant resources from ADM(PA), and duplicated effort as MilStratCom sought to create their own capabilities and products such as information environment assessments. For several years, this also affected the ability of the ADM(PA) Group to support the breadth and scope of ongoing DND/CAF operations and activities, including during the first year of the pandemic.

[42] Canadian Armed Forces, Military Strategic Communication and Public Affairs Operationalisation Force Development Plan, 16.

that scored the lowest was for Capt. Jones to wear an armband, badge or other visible identifier so journalists would see that officer was engaged in traditional, truthful communication. This was assessed as not significantly bolstering perceptions of credibility and had no impact on operational effectiveness but was cheap to implement.

A second option considered moving PA-trained Capt. Williams to a separate branch with instructions not to interact with media for the duration of the posting; afterwards to rebadge back to PA. This was assessed to "significantly bolster perceptions of credibility" but came at the cost and effectiveness of managing multiple small branches and so ranked second. A third option considered three distinct branches – military PA, imagery and information effects (IO), all with unique cap badges and branding – with those in information effects not to "officially engage with media." This was also assessed to significantly bolster perceptions of credibility and scored the highest of the three prospective courses of action. A fourth option, preferred but not scored, suggested a CAF information branch with military PA, imagery, information effects (IO) and PSYOPS components.[43]

This was not brainstorming about how to build bridges to enable greater co-ordination of effort on active operations, but an express intent to tear down firewalls. It was a foreshadowing of events to come.

The MilStratCom Initiative Proposition

During its 2015-2020 lifetime, the initiative was referred to variously as CAF StratCom (up to early 2018), MilStratCom (up to summer 2019), Military Public Affairs (MilPA, up to November 2020) or PA Operationalization more generally, with different formulations interchangeably being tried. Each fell into disfavour one by one: the term MilStratCom was used most often. In the absence of initial overarching written senior leader guidance and full-time staff at first, work to name the effort let alone define the requirement and set out a plan percolated slowly for the first two years. The initiative was socialized for the first time to senior CAF leadership at Armed Forces Council in September 2017 and offered real promise.

The pitch was that adversarial information campaigns were strategic in design and scope, conceived and authorized by political decision-makers to divide allies, disguise intent and attribution and disrupt democratic societies using information advantage to overcome military inferiority. The problem, as laid out for Armed Forces Council, was threefold: military PA was created 40 years ago as an ancillary (support) service; the PA function was under civilian management and this led to an "erosion of operational relevance"; and gaps included "no operational social media capability."[44] In response, the CAF needed a strategic approach to

[43] National Defence, Military Strategic Communications, Topic 2: Courses of Action for Distinguishing PA vs StratCom Practitioners, undated presentation, likely 2018 or 2019.
[44] Brigadier-General Marc Thériault, "From Operationalizing Military Public Affairs to Enhancing CAF in the Information Domain," brief to Armed Forces Council, September 8, 2017. (See ATIP A0557002).

building, enhancing and synchronizing the full spectrum of information-related capabilities. The effort would be pan-military, drawing on various offices to lead reform efforts in their respective areas of responsibility, including IO modernization with the chief force development staff; targeting, which implicated numerous groups including intelligence; building up the army's 10 influence activity companies; establishing a joint operational effects cell at Canadian Joint Operations Command (CJOC); the military Public Affairs operationalization/MilStratCom effort; and, a separate PA transformation initiative at ADM(PA).

Together, it was argued, this organizationally undefined collection of new and improved capabilities would dramatically improve outputs like the CAF's information environment analysis capability, drawing information from social media, media reports, polling and open-source intelligence to be fused into actionable reports. This insight would better inform processes to identify adversary, audience or actor targets, and help decision-makers match the right inform-influence-persuade-coerce capability to the specific target to achieve a desired effect. At issue though, in lieu of a new purpose-built entity to lead the effort, which existing group could do so?

Only Public Affairs had a cadre of experienced professionals operating as a joint, all-services asset and with significant extant capacity. After all, the ADM(PA) functional authority had more than 950 staff, including: imagery technicians nested throughout the DND/CAF chain of command across the country; ownership or control of many of the internal and external communication platforms; considerable information environment assessment capability; a career classification for practitioners (unlike IO and PSYOPS), meaning experienced practitioners served at each rank from lieutenant to colonel; an established training school; relevant administrative order and directives defining how the function worked; authority to provide direction and guidance for all public communications by Defence; well-practised approval processes, however clunky at times; and a well-established, formal chain of command with ADM-level representation to the CDS and DM. These were formidable assets, if only they could be "made more military and focused on CAF imperatives, and less focused on institutional interests," in the words of one MilStratCom team member.[45]

There was no designated overseer of Defence StratCom or IO,[46] no written senior leader directives, no existing structure to naturally park this type of work and weak governance mechanisms to help prioritize and steer the effort as it advanced. The work was considered an operational problem of insufficient process, and so it was thought there was no need to conceive of it as a formal project that needed to be strictly managed at the strategic level. Only one capability really wanted the lead and had some capacity to immediately take it forward: although PA was not officially designated the MilStratCom initiative champion, the CAF senior leader consensus expressed as verbal commanders' intent was clear – PA could proceed as such, unless told otherwise. To better effect this, the senior PAO, Col. Marc Thériault, had earlier been promoted to brigadier general, in a first for the PA branch. His successor, Col. Jay Janzen, followed that trend in early 2018 when

[45] Interview with a senior officer practitioner, fall 2021.
[46] In April 2018, the Strategic Joint Staff/director of staff was named in policy as the functional authority for IO, an entirely impractical situation given the importance of that office to all aspects of CAF business and their intense workload.

Thériault was seconded to then-Governor General Julie Payette's office) and a former senior military PAO was appointed as the civilian ADM(PA), the top communications job at DND.[47]

The approach was to create a team within ADM(PA), focused on CAF StratCom (changed to MilStratCom, then to MilPA). The immediate resource ask was for 47 people, a mix of new positions and reallocations from within ADM(PA) over three years, with expectations of further growth.[48] When fully operational, this was meant to establish four deployable "cognitive domain teams," enhance readiness of practitioners, provide more robust information environment analysis, more operational imagery and support the joint targeting effort. When deployed overseas, the PA teams would operate "under the auspices of a wider InfoOps framework." In Canada, the group would "operate in close coordination with Defence and [other government department] Public Affairs" but would be physically and organizationally separate. Multiple lines of effort were detailed for initiatives along four tracks: develop resilient military communications professionals, design new capabilities and leverage technology, adopt new structures and processes, and support CAF-wide efforts "to enhance internal mindsets."[49] Many of the proposed outputs were already being done within ADM(PA) or improvements in train, but these proceeded slowly and with a civilian flavour, and were not considered fit-for-military-purpose: the proposed plan was one that could scratch the itch of operators and military practitioners alike.

The Problem Set – Dangers of Situating the Estimate

The frame of reference informing the initiative from the start was this: Canada and NATO were at undeclared war against malign state and non-state actors seeking to upend the rules-based international order. To meet this challenge, DND/CAF – but the CAF in particular – needed to evolve the way in which it generated its military forces and equipment, including in the informational space. This effort needed to start now, without delay. Further, the view was that for too long, DND/institutional communication needs had taken precedence and a rebalance of resources, focus and staff was in order.

With the verbal support of the CDS to weaponize/operationalize PA, these efforts could proceed with some urgency, and without the usual written guidelines such major efforts would usually require, such as a CDS initiating directive. The effort was fourfold: to build small teams, including with imagery capability that could more readily deploy on contested overseas operations or in conflicts; to conduct more extensive target audience analysis to inform the CAF joint targeting effort; to develop information warrior practitioners, including by exposing and embedding PAOs more deeply into the influence-focused courses offered to IO and PSYOPS and to make PA training more widely available to them; and to "maintain NATO/Allied perceptions of CAF leadership in advancing StratCom."[50]

[47] Capt.(N)(Ret'd.) Chris Henderson served as ADM(PA) from October 2017 to December 2019.
[48] Canadian Armed Forces Military Strategic Communications/Public Affairs Force Development Plan, 18.
[49] MPAEEC, 12.
[50] CAF StratCom Force Development Plan. PowerPoint presentation, September 2019.

Core activities that were time consuming, like improving governance, conducting training needs assessments or evolving outdated DND policy and regulations were considered an institutional/DND remit under a broader ADM (PA) transformation effort, and not the responsibility of the MilStratCom group.

The decision by DND/CAF leadership to allow the initiative to proceed without first putting in place a trusted project management methodology, including establishing objectives or a requirement to regularly report to an effective senior leader oversight body allowed a cluster of work strands to operate without sufficient guidance.[51] Normally, initiative leads would have first validated in detail the baseline, taking stock of the status and condition of all related policy, doctrine, means of governance, training needs and resources (who owns what, where is it and how much) in all information-related capabilities.[52] This was not done, allowing pre-conceived operator and practitioner mindsets and hasty assumptions about underlying issues and challenges to stand. After all, as the MilStratCom lead claimed in one early assessment to senior CAF leaders: "Only 2-3 actors are likely to publicly oppose CAF MilStratCom efforts. Actors may oppose these efforts *regardless of the content*. Arguments will be *dispelled and not gain traction*" (emphasis in the original).[53]

Three other examples (policy, benchmarking and training) are worth brief mention to understand how the initiative got off track from the start. First, the Queen's Regulations and Orders (QR&Os) have the force of law in the CAF and those governing the DND/CAF communication function are more than two decades old – with much quaint language harkening back decades further.[54] Of the overarching Defence administrative orders and directives (DAODs) establishing how the public affairs function works at DND, six of the extant nine are the originals from 1998 – including PA planning, media relations and internet publishing.[55] Thus, the communication-related laws,

[51] Reform efforts of this size, scale and scope would normally start with articulation of a project management charter or CDS initiating directive setting out the overall aim and goals and detailing roles and responsibilities. This did not happen. A substantive effort toward this took place only in November 2020, a week after the MilStratCom initiative was cancelled, via guidance issued by the CDS and DM called Resetting the Various Information-Related Capabilities. The 2011 Report on Transformation (the Leslie Report) was an obvious, effective model that could have informed a work plan: identify and appoint a seasoned leader with a written mandate; collect and aggregate data and interview extensively to fully grasp the baseline situation, research who else was doing it better and why and make deductions about which issues needed to be fixed.

[52] For instance, there are more than 950 military and civilian positions in Defence Public Affairs and/or under ADM(PA)'s functional authority, and in the army there are 10 influence activity companies (this is a unit designation, not indicative of actual size, a company normally being around 80-120 people). The 950 figure includes 196 regular force PAOs, 115 reserve force PAOs, 301 in the civilian information services category, 266 in the imagery trade and nearly 120 others using staffing mechanisms such as term, acting or casual assignments, plus support staff (Source: DND Media Liaison Office email, December 23, 2021). Knowing these data ahead of time may have suggested a key issue was not a lack of people, but an organizational design and allocation problem.

[53] National Defence, CAF StratCom Force Development Brief. PowerPoint presentation, September 2019.

[54] Per QR&O 19.36: no CAF member without permission can "deliver publicly, or record for public delivery, either directly or through the medium of radio or television, a lecture, discourse or answers to questions relating to a military subject." Other highlights include that no CAF member can "publish in any form whatever any military information or the member's views on any military subject to unauthorized persons"; "prepare a paper or write a script on any military subject for delivery or transmission to the public"; "publish the member's opinions on any military question that is under consideration by superior authorities"; or, "take part in public in a discussion."
See: https://www.canada.ca/en/department-national-defence/corporate/policies-standards/queens-regulations-orders/vol-1-administration/ch-19-conduct-discipline.html. Accessed January 10, 2022.

[55] There are nine DAODs in the 2008 Public Affairs series: -00 Public Affairs Policy (1998);
-01 Accountability and Responsibility for Public Affairs (1998); -02 Media Relations and Public Announcements (1998); -3 Issue and Crisis Management (2003); -4 Public Affairs, Military Doctrine and Canadian Forces Operations (1998); -5 Public Affairs Planning and Program

policy and planning framework are more than 20 years old and are not fit for purpose for military operations in the modern-day information environment. Updating these is time-consuming and detail-oriented work. Identifying these early on as a MilStratCom initiative need and lead would likely have avoided missteps to come respecting operational policy (the subject of Chapter III).

Second, research to obtain a solid understanding of organizations to benchmark (who is doing this well now, and why is that) would have made clear the characteristics that work in each and could expect to be successfully imported, and those not likely to succeed. NATO HQ Brussels, the U.S. Marines, and the U.K. military are noteworthy examples of success:[56] from the perspective of a state-on-state contested conflict we would now add the Ukrainian government/armed forces. Notably, such research would have identified that the term "IO" was being progressively weeded out of military organizations including the U.S. military, with the Marine Corps and the Joint Staff, the leading thinkers on the subject in that country, preferring the term "operations in the information environment."[57] "Far from a semantic matter of definitions between services," wrote American practitioners, "this issue directly affects the ability of the [U.S.] armed forces to effectively counter hostile influence efforts…" [58]

Third, the key to reform of a CAF trade or occupation is an occupational analysis, a formal process to annotate and validate all the various tasks, skills and knowledge that people at each rank level in each job in that profession need to know. This determines training needs. The occupational analysis for PA did not begin with the MilStratCom effort in 2015, but only in earnest after the initiative was cancelled in November 2020. The complementary effort for the IO component was, oddly enough, led by CJOC, the army having gratefully given up responsibility for doing it on the grounds of insufficient resources. Identifying and prioritizing this critical need for all the affected

---

Delivery (1998); -06 Internet Publishing (1998); -08 Official Use of Social Media (2018); -09 Public Opinion Research (2019); -07 Canadian Forces Parliamentary Program is cancelled. See https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2008.html. Accessed January 10, 2022. It is not at all clear how QR&Os and DAODs might, could or should apply to other inform-influence-persuade capabilities such as IO and PSYOPS in the internet age.

[56] In this author's opinion, NATO HQ Brussels is a model for excellence in large international institutional communications, and the U.S. Marines the example of choice for a "single Service." In terms of specific countries, the U.K. has made major inroads with innovative policy (Joint Concept Note 2/18 Information Advantage and Joint Doctrine Note 2/19 Defence Strategic Communication*:* An Approach to Formulating and Executing Strategy); leading-edge organizational change including a Strategic Command headed by a four-star general; subordinate HQs like 6 (U.K.) Division and 77 Brigade, specializing in media operations and influence; an infusion of experienced senior military operators doing communications; a serious upgrade in digital content online especially in the U.K. army; and major investments to inculcate an operational mindset change toward the integration of information into its operations and activities. The U.K. military initiative also benefited from the active support of world-class think tanks such as RUSI and Chatham House providing external expertise, and longstanding relationships with major universities such as King's College with its own Centre for Strategic Communications. The situation in the U.K. was informed by serious, mature parliamentary examinations of operational lessons learned particularly from the Iraq conflict, and of fake news/disinformation. Importantly, the U.K. also bore actual experience of a major influence and disinformation campaign by Russia (the 2018 poisoning of the Skripals) that overtly alerted the nation to proof of malfeasance afoot by a foreign power. None of these important factors for success applies in Canada.

[57] In 2017, the U.S. military recognized information as the seventh joint function (alongside command and control, fires, intelligence, movement and manoeuvre, protection and sustainment), and in 2019, the U.S. Marine Corps recognized information as its seventh war-fighting function (alongside command and control, fires, force protection, intelligence, logistics and manoeuvre). The U.S. Armed Services also benefited greatly by hiring a major think tank like RAND to assist with IO-related policy development.

[58] Daniel de Wit and Salil Puri, "Finding the Right Words: Ending the Confusion on What 'Information Operations' Actually Means," *Small Wars Journal*, May 14, 2021. A considerable amount of U.S. military literature is devoted to this very subject. Two other articles that cover the issues well are Christopher Paul, "Integrating Apples, Oranges, Pianos, Volkswagens, and Skyscrapers," *IO Sphere: The Professional Journal of Joint Information Operations*, Winter 2014, 3-5; and Christopher Paul, "Is It Time to Abandon the Term Information Operations?" Commentary, *Strategy Bridge*, March 13, 2019.

information-related capabilities up front at once and as a joint project would have meant the work would have been complete by 2018, and informed actual training and resource decisions from that point, or even sooner.

In sum, the MilStratCom initiative started the complex problem set by looking through the wrong end of the telescope: allowing this was a failure mainly by senior CAF leadership. The requirement was for a top-down enterprise-wide strategy agreed to in writing by senior DND/CAF leaders, led by an experienced general/flag officer operator or equivalent official, in charge of a full-time project team with representation from the associated capabilities to examine all facets of how to enhance support to domestic and international requirements. Instead, the initiative was encouraged as a series of bottom-up tactical activities mostly about PA and led by PAOs, with a focus on overseas, contested operations instead of a balanced approach along with domestic requirements, with little oversight and even less governance. This sclerotic mindset and operator culture set the conditions for how the MilStratCom initiative was to unfold and expressed itself in various draft policy documents that inevitably led to a number of public missteps affecting organizational credibility and institutional reputation.

It is a truism that the military plans and trains hard for war, so that operations during peacetime are easy. For PA and StratCom, the obverse is the case: peace is hard, but war/conflict/tension is comparatively easy. Russia is making claims about our troops, NATO intentions, war aims and outcomes? That is overt disinformation, and despite the "hybrid war is new" enthusiasts, this has been standard operating procedure for decades.[59] In the case of contested operations such as against Daesh, the reason for fighting a murderous band of religious zealots trying to kill us is not exactly a tough counter-narrative to construct, with success made easier by retaking the territory they once controlled. It is considerably more difficult to enrich domestic audience understanding about such things as future major equipment procurements; the reasons for modernizing NORAD and why that's expensive; explaining how the institution is tackling culture change; and, why the CAF deploys to where it does.

That is, the capacity and capability to conduct superb, trusted 24/7 institutional and operational communications supported by DND/CAF practitioners is the best foundation to serve domestic requirements, all expeditionary outside-Canada contested operations and to tackle malign-actor activities in the grey zone.

The next chapter examines the evolution of key CAF draft policies and how the imbalance of CAF thinking and effort between domestic and international activities weighted to the latter, with its lexicon specific to contested operations but used in a domestic context, ultimately derailed the MilStratCom initiative.

[59] See Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare.* (New York: Farrar, Straus and Giroux, 2020); and Keir Giles, *Moscow Rules: What Drives Russia to Confront the West (*Washington*:* Brookings Institution Press, 2019).

Table 1: Addressing the Problem Set Has Been Hobbled by Many Myths – A Top 10 List

The Operating Philosophy of the MilStratCom Initiative vs. the Reality

1	*Hybrid warfare/grey zone/Phase 0/Below-threshold level of conflict is new.* No. Hybrid war techniques are ancient and used by all sides. What's new is how easy it is now to create content at scale, speed and amplified with global reach plus real impact; and the massive investment by malign actors in order to make and distribute mis- and disinformation.
2	*Communications reform needs to focus on contested conflict among nation-states, using a war-based lexicon (non-munitions capabilities, targets, adversary, threats), even in a domestic context.* No. The loss of public faith and trust in government and institutions is the key fight and a suboptimal communications function is potentially an existential threat to the DND/CAF. Satisfying the home front means right communications policy, doctrine, structure, capabilities and practitioners: do this well and supporting contested operations is comparatively easy. And, lexicon matters.
3	*The CAF should ethically influence Canadians to generate desired effects; practitioners who do not support this concept are corporate PR agents who don't understand the operating environment.* No. Applying this dangerous tenet to Defence Public Affairs would mean the public and media would never trust DND/CAF communications. Instead, consider "proactively inform" or "principled persuasion."
4	*In Canada, operational (CAF) and institutional (DND) communications should be organizationally separate, only needing to work in close co-ordination.* No. These are not mutually exclusive undertakings, but two sides of the same coin.
5	*The CAF needs to foster an information warrior culture among military practitioners.* No. The ideology behind "warrior" in this context is misplaced. The DND/CAF needs professional, exceptionally competent practitioners who are a part of, not set apart from, society.

6	*The young folks we have who are keen on understanding the information sphere and then using these sorts of tools … we don't restrain that sort of initiative.* No. The CAF does and must restrain that sort of initiative and ensure actions are guided by explicit authorities, oversight and training. Doing otherwise will ruin DND/CAF credibility and reputation.
7	*The Defence mandate gives operators Crown prerogative to conduct IO, which is applicable to all defence activities and operations, including in domestic applications.* No. What's fine for use overseas against malign actors and in domestic applications needs to be made much clearer in policy. Instead, evolve the DND/CAF mindset to more effectively embed information effect considerations in operational planning and decision-making from the start.
8	*The IO problem is a lack of delegated authorities for activities other than conflict: we need to shift from a responsive to an anticipatory posture vis-à-vis policy, authorities, mandates and capabilities.* No. Nearly all DND/CAF StratCom problems are a result of suboptimal policy, questionable leadership decisions, poor execution or lack of communications effort – usually two or more. Rarely is a lack of authorities the reason for suboptimal outcomes.
9	*IO and PSYOPS staff reporting to PAOs within Defence Public Affairs is good MilStratCom.* No. This harms the DND/CAF's reputation and credibility. Defence communications needs to be re-imagined, and based on excellent, expanded PA capability. The IO function and PSYOPS are not fit-for-purpose and both need to be repurposed and re-organized, not expanded.
10	*The motto "who dares, wins" is as applicable to strategic communications as it is to warfare.* No. This appropriation from the U.K.'s Special Air Service is misguided. The consequences of unbounded "take a chance, go for it" communications and actions even by well-meaning practitioners or leaders at tactical, operational or strategic levels can have very serious repercussions.

III: Problematic Policy Foundations Become Entrenched

This chapter describes the key information-related policies that bore on the MilStratCom initiative, how these evolved and why, as a result, failure was inevitable. The quest to evolve military policy, doctrine, organization structure and capability to improve operational outcomes for Defence through more co-ordinated use of all its tools to inform, influence, persuade and coerce began in mid-2015, shortly after Vance became chief of the defence staff (CDS). Vance had a unique-to-the-top-job combination of deep and meaningful command experience in active combat and conflict from tours in the Balkans and Afghanistan, and assignments in key, tough staff positions in Ottawa. He had seen up close on operations how insurgents and malign actors skilfully manoeuvred in the informational space and was familiar with the comparative shortcomings of Canadian military capability as well as the opportunity and need for doing notably better. Overtly calling for change so soon in his tenure suggested a welcome new understanding of the central importance of strategic communications to military operations and activities in the modern information environment.

At this early juncture, the initial focus – thought to be low-hanging fruit – was to improve the DND/CAF public communications effort on overseas deployed operations on combat, during lesser conflict and in below-threshold reassurance and deterrence missions such as the CAF deployment in Eastern Europe (Latvia, Romania and pre-2022 war Ukraine). It was expected this would also accrue benefits for the home game. The main line of effort, though, was decidedly in support of combat, low-intensity conflict or near-conflict missions overseas. Hence, the initial characterization to "weaponize" Public Affairs. [60]

Vance's "commander's intent" was expressed only verbally (first articulated in writing more than five years later in November 2020 by Vance and then-deputy minister Jody Thomas) and was quickly met with criticism and skepticism by some media who regularly covered Defence. This reaction was an expression of frustration with what some journalists considered to be a pattern of less-than-forthright public communications and a confrontational approach by Defence

[60] See David Pugliese, "Chief of the Defence Staff Gen. Jon Vance and the 'Weaponization of Public Affairs,'" *Ottawa Citizen*, September 21, 2015, https://ottawacitizen.com/news/national/defence-watch/chief-of-the-defence-staff-gen-jon-vance-and-the-weaponization-of-public-affairs. Accessed January 10, 2022. The "weaponization" of Public Affairs, a term used infrequently and quickly changed to "operationalization," was an unfortunate characterization that encumbered the reform effort right out of the starting blocks. "Weaponization" inferred that everyone was a "target" subject to prospective attack and that Defence communication was a one-way fire-for-effect discharge, not a two-way conversation. It also evoked the prospect of random, unbounded use of capabilities unique to the military to overtly influence and coerce and could result in collateral damage – in this form, affecting reputation and credibility. The term, left uncorrected, also framed the broader institutional and operational information-related capability reform challenge as one related to fixing process, structure and practitioner training just in Public Affairs. The deliberate PA strategy was to ignore the story and subsequent articles by Pugliese, *Esprit de Corps'* Scott Taylor and others about the subject, hoping the coverage would be a one-day thing. From the start, Public Affairs staff had convinced decision-makers in Defence not to actively engage media about the subject on the grounds the attention was from just a disaffected few, long-time critics of military Public Affairs, and that other journalists and the general public would neither notice nor care. This odd strategy continued for the duration of the project even as negative coverage mounted. Dozens of stories later – see Appendix 2 for headlines just from 2020-21 – "weaponization" as a reference frame, and the decision to not provide context and perspective to explain the reform effort, helped sink the initiative. The term was even used five years later in November 2020 by Opposition defence critic James Bezan (Figure 6-1), a good illustration of the long shelf life and impact of a negative narrative frame left unexplained.

practitioners to media critical of DND and in particular of the military. Many serving Public Affairs officers also expressed concern internally of what was thought to be an underlying motive to shift from the traditional inform function to engagement in IO and PSYOPS activities.

As discussed in chapter II, Public Affairs was simply one discrete, tangible line of effort in a bigger, more ambitious aim to develop a planning concept and the means to align all Defence actions, images and words to achieve desired outcomes. A broader DND/CAF strategic communications vision was yet to be articulated and remains the case even today, more than six years after the initiative began.[61] The CAF did not, and does not, have overarching policy or the organizational structure to readily assign such work – unlike for example in the U.K., with its Strategic Command headed by a four-star general and constituent parts including 6th (United Kingdom) Division and 77 Brigade, both tailored for information advantage activities and information warfare. Nor was there a champion or functional authority for IO at the time, let alone for StratCom. Since much of the senior leader angst about StratCom related in some way to public communication, and with no obvious place to park the effort, by default ADM(PA) assumed tacit lead with the support of senior leadership and began to develop the overarching concept.[62]

Strong, Secure, Engaged (SSE) Defence Policy (June 2017)

The desire to develop a broader array of fit-for-purpose information-related capabilities for offensive purposes during conflict or during times of tension but less than war, was identified in the June 2017 *Strong, Secure, Engaged* (SSE) defence policy. The policy is heavy with context for major kinetic equipment purchases and light on the impact of the information environment on modern-day operations, with even less said about public trust and its impact on organizational credibility and institutional reputation. This was a missed opportunity to articulate the need for eliminating potential confusion about StratCom reform in a critical document that was bound to stand for several years.

One of the key initiatives that flew under the media and public radar was the SSE's intent to develop "military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence and attack in support of military operations."[63] The defence policy also sought to "enhance existing roles assigned to Reserve Force units and formations" including giving them the lead to provide trained personnel for information operations and influence activities, including PSYOPS.[64] The types of tasks this capability might be called to do were not

[61] In a June 2021 directive, the CDS and DM tasked the joint staff to prepare and issue a Defence StratCom initiating directive by November of that year, thereby clarifying Defence intent. As of February 2022, this remains a work in progress.
[62] Marc Thériault, "Conceptual Vision: From Operationalizing Military Public Affairs to Enabling the Canadian Armed Forces in the Information Environment." By January 2018, some PAOs including Col. Jay Janzen, who would soon be the senior ranking officer in Public Affairs, had adopted and were using the MilStratCom title, signalling to all parties a desire to be seen to be driving the overall effort, even if not explicitly tasked.
[63] *Strong, Secure, Engaged*, initiative 65.
[64] *Strong, Secure, Engaged*, initiative 76. This meant army since neither the RCAF nor the RCN had these capabilities. Relying on the reserve force to recruit, train and manage (force generate) practitioners in this area, is by a large margin the least effective way possible to do so, and the decision to double-down on this approach guaranteed suboptimal outcomes. The extremely limited application in Canada for IO and PSYOPS;

explicitly set out, but were hinted at by then-Defence minister Harjit Sajjan, who wrote in his cover letter that, "The distinction between domestic and international threats is becoming less relevant." This was a public admission that Canada was going to be more actively engaging in the informational space in a more deliberate way.

The SSE called for the creation of a cyber-operator occupation, up to 300 new positions in the intelligence branch and a serious upgrade to CAF intelligence, surveillance and reconnaissance capabilities. These were key to better know and understand what was happening in and around the land, sea, air, space and cyber-domains of the world's second largest country. The defence policy also made clear this situational awareness was central to the "targeting process" – a formal, deliberate approach to help commanders decide how to select and prioritize targets and determine "the most effective way to deal with them, whether through lethal or non-lethal means."[65] The SSE policy was the catalyst to evolve the process and use of "targeting" in CAF activities and operations. Later, this language would prove problematic when applied to all military activities, suggesting that Canadians and allies – lumped together with terrorists and other malign actors – were simply targets, ripe for engagement with "non-munitions activities."

MC 0628 NATO Military Policy on Strategic Communications (August 2017)[66]

One development on the international policy scene had particular impact on the Canadian MilStratCom experience and the timing was important. After considerable discussion at NATO spanning nearly a decade, in August 2017, the North Atlantic Council endorsed a NATO Military Policy on Strategic Communications (MC 0628).[67] The policy-drafting effort and negotiation with national representatives over each word had been driven mainly by the two strategic NATO military commands.[68] This was a milestone in the evolution of an often fractious debate: strategic communications as an operating concept had come into its own with actual policy agreed upon by military and political authorities; Military doctrine could then be developed and, at least in NATO military HQs, a grouping of, and hierarchy between, information-related capabilities/functions had been achieved.

---

the lack of policy, doctrine and training opportunities; the modest level of relevant experience of practitioners and commanders; the high consequence of error; and no career field prospects lends itself poorly to a single-service reserve model. The initiative was included in the *Strong, Secure, Engaged* section: "A New Vision for the Reserve Force" and not "investments in joint capabilities," a sign the intent was not to expand the skill set to the RCAF and RCN, though these services of course also conducted expeditionary operations on a regular basis.

[65] *Strong, Secure, Engaged*, 66. "Lethal" being self-explanatory; "non-lethal" being the nearly infinite number of signals and actions that can be taken to coerce, threaten, influence, persuade or otherwise incentivize desired behaviour.

[66] Notably, not a NATO policy on military strategic communications. As a military committee document, within the various NATO headquarters MC 0628 was inherently understood as policy that related to military considerations and applied to NATO military headquarters in particular. In Canada, the choice of lexicon was MilStratCom, which sent many down a deep rabbit hole. The distinction at first blush may seem to be one of semantics but military StratCom and military PA imply that the distinctive qualifiers "civilian" or "political" also exist. This choice of framing led to a deliberate effort to separate the military/operational communicators from the mostly civilian/institutional communicators to protect the former from influence of the latter. The choice exposed a long-simmering condescending attitude by some military practitioners toward their civilian counterparts and of civilian leadership, who served under different terms of service than CAF members.

[67] Cover letter by Gen. Markus Kneip, Chief of Staff SHAPE, to Memo, *NATO Military Policy on Strategic Communications*: August 14, 2017.

[68] Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium and Allied Command Transformation in Norfolk, Virginia. See Mark Laity, "The Birth and Coming of Age of NATO StratCom: A Personal History," in *Defence Strategic Communications Journal*, (NATO Strategic Communications Centre of Excellence, vol. 10, Spring-Autumn 2021).

The policy's main take-away was the overt expression that the mindset of military planners and decision-makers needed to change so that communications considerations would be more deliberately integrated into all decisions about military activities, including and especially at the planning stage. To facilitate that, the policy directed an organizational change at NATO military HQs to combine the communication capabilities and the information staff function – StratCom, Military Public Affairs, Info Ops and PSYOPS – into a stand-alone group under a director of communications. This individual, reporting to the Command Group, was given authority to direct, guide and co-ordinate the overall communications effort.

This structure makes practical sense at NATO military HQs in static locations like Mons (Belgium), Norfolk (U.S.), Naples (Italy) and Brunssum (the Netherlands), and on deployments like the ISAF/Resolute Support Mission in Kabul. NATO military HQs have representatives from as many as 30 Alliance members and sometimes nearly as many partner nations, with multiple languages and cultures at play. Very few militaries have full-time career specialists in the information-related capabilities, and so the related skills and experience of practitioners and even senior officers' experience managing or interacting with such functions is highly variable.[69]

Not all NATO member nations have the same appreciation about the role and place of a critical, independent media in society nor provide the same media access to their military forces as Canada, the U.S. or U.K. NATO's information classification is strict and the ability to publicly release NATO information is very challenging. On contested operations such as in Afghanistan with nearly 250,000 military and contractors from 50 nations at its peak, there are many overt, publicly competing national agendas at play. In such circumstances, a firm grip of the communications function through a director or chief of strategic communications is a necessary tool to effect better co-ordination of communications activities and reduce the prospects of information fratricide.[70]

Conversely, for a variety of reasons, that organizational structure does not work at National Defence Headquarters (NDHQ) in Canada. The operating environment at a NATO military HQ is vastly different from that at a national, strategic, political-military HQ under the regular glare and scrutiny of ministers, Parliament, the media and subject to the *Access to Information Act*. Simply put, SHAPE HQ Mons is not NDHQ Ottawa. Thus, the move by the MilStratCom group at ADM PA to import the NATO military HQ communications model, including several IO and PSYOPS staff in the PA structure within the ADM(PA) Group, shattered the longstanding policy, convention and practice of an appropriate firewall between PA and the other capabilities involved in deception and outright influence.[71]

[69] For instance, the Canadian multinational battle group as part of NATO's enhanced forward presence in Latvia has under command (as of January 2022), personnel from Albania, Czech Republic, Iceland, Italy, Montenegro, Poland, Slovakia, Slovenia and Spain. See https://www.nato.int/nato_static_fl2014/assets/pdf/2022/1/pdf/220104-MAP-eFP-en.pdf. Accessed January 10, 2022.
[70] See Brett Boudreau, "NATO's Information Campaigns in Afghanistan, 2003-2021," in *From World War 1 to the Twitter Era* (Boulder, CO: Lynne Rienner Publishers): 117-168.
[71] ADM PA/CF Strategic Communications Group organization chart, September 4, 2019.

DND/CAF Policy on Joint Information Operations (April 3, 2018)

Spring 2018 was a watershed period in the evolution of the MilStratCom initiative. In April 2018, Vance and Thomas signed the DND/CAF Policy on Joint Information Operations, an effort to translate the *Strong, Secure, Engaged* intent into actionable policy and work around the shortcomings of the seriously outdated Canadian army IO doctrine from 1998. The new policy was a rehash of old Canadian doctrine and drew heavily from that more recently agreed upon by NATO.[72]

The Joint Info Ops Policy had three key features. First was the assertion that the defence mandate granted Crown prerogative, meaning the "DND/CAF may employ Info Ops in support of defence activities and operations," and that the policy "is applicable to all defence activities and operations." The policy directed that Info Ops be incorporated "in the earliest stages of planning and throughout the conduct of operations" and was in fact "already an element within the CAF targeting enterprise." This demonstrated a major misunderstanding of the application of Crown prerogative that cabinet ministers traditionally exercise.

Second, the Joint Info Ops Policy clearly stated the CAF "may conduct operations *within Canada* in accordance with the defence mandate" – meaning a domestic application – but did not exclude use of capabilities for the intent of deception, influence or coercion. Third, the Canadian Joint Operations Command (or CJOC, responsible for all operations domestic and otherwise), Special Forces Operations Command and NORAD commanders were force employers and thus, "shall…integrate Info Ops into operational planning."[73] The responsibility to oversee this – recalling that "everything" is information – was the Strategic Joint Staff/Director of Staff, one of the busiest offices in the CAF.[74]

The document is an information operations practitioner's dream – but a policy minefield and a strategic liability for the DND/CAF. The policy does not sufficiently differentiate between domestic and international/contested operations regarding the use of military intelligence, the Communications Security Establishment, PSYOPS or offensive cyber- or military deception. It also sets out ambiguous authorities based on a loose interpretation of Crown prerogative that could potentially lead to the conduct of seriously invasive activities by staff acting in what they believe to be the defence of Canada.[75] The Joint Info Ops Policy was now on the street, giving oxygen to practitioners looking to test the limits of what the new market could bear, and played a central role in unfortunate events to come.

---

[72] MC 0422/5 NATO Military Policy for Information Operations, September 5, 2014. The "5" designation means this is the fifth iteration of said policy, an indicator of the challenge within NATO militaries to settle on an agreed concept.
[73] DND/CAF Policy on Joint Information Operations, April 3, 2018.
[74] This decision attests to the lack of functional structure or governance mechanisms within the CAF to appropriately oversee and manage the breadth of information-related capabilities. In effect, this left the initiative, including its various strands and many different leads, to proceed along individual tracks with a minimal amount of oversight to steer them right.
[75] In June 2021, acting CDS Lt.-Gen. Wayne Eyre and DM Thomas issued direction to publish an updated Joint Info Ops Policy by November 2021, to "more clearly identify and delineate policies, doctrine and directives relating to domestic operations." (Discussed later in Chapter V). As of April 2022, that remained a work in progress.

Public Affairs Tweet Storm and 'Ethical Influence'

In February 2018, senior PAO Col. Jay Janzen complained to Global News via tweet (Fig. 1-1) about Col. (Ret'd.) Michel Drapeau's media commentary concerning Tiger Williams being charged for sexual assault stemming from an incident in December 2017 while travelling on a CAF-sponsored morale-boosting visit to troops in Greece and Latvia.[76] In his Twitter profile picture, Janzen appeared in uniform but claimed to be expressing personal views, prompting internal discussion at DND about the appropriate limits for social media use by attributed CAF officers (a tricky issue and still generally unresolved in relevant policy).

On April 3, the day the Joint Info Ops Policy was issued, again by tweet (Figure 1-2), Janzen equated long-time journalist Scott Taylor to a Russian propagandist, an overt coercion tactic aimed at him and two of the reporter's employers. This was not just an indecorous riposte at a journalist who for years had taken contrarian views to the official Defence line on many issues, but implied the reporter was a national security concern.[77] With more and more threats aimed at reporters in the U.S. and Canada, this potentially put Taylor's physical and financial security at risk. A week later came another tweet (Fig. 1-3), expressing frustration about the media's use of the *Access to Information Act*, which often resulted in uncomfortable media articles about Defence.

Later that month, and little more than two weeks after the Joint Info Ops Policy was issued, the same officer tweeted that the ongoing parliamentary debate and media discussion of the prospect for combat during the CAF deployment to Mali was "nonsensical" (Figure 2-1). This, even though the UN had recently published statistics showing that for the fourth year in a row, peacekeepers in Mali suffered the highest loss of life due to malicious attacks, of any of the UN missions.[78] The commentary led to an angry rebuttal on Twitter by Opposition critic James Bezan (Fig. 2-2, and displaying a long memory, eight months later by Erin O'Toole – Fig. 2-3), and led to several media articles about the exchange. Janzen explained that his rationale for engaging and for suggesting "better" questions was to encourage public discussion about the CAF, though Defence did not hurry to answer the questions posed.

The overt public criticism of media and critics by the top military Public Affairs officer, and actions by colleagues to pressure media organizations to take action against reporters over their coverage, looked to be a deliberate, if ham-fisted influence strategy, and was destined to backfire. The tweet storm – as it came to be known inside PA circles – that in short order tagged and criticized just about every reporter regularly covering Defence, marked a new low in post-Somalia scandal

[76] The "party flight" and the many Public Affairs missteps in handling the issue provided the *Ottawa Citizen's* David Pugliese with regular material about how explanations by DND of what happened were judicious with the facts. The "party flight" stories riled Defence leadership and PAOs like no other and led to efforts to take action against the reporter. See David Pugliese, "20 DND Staff Involved in Writing Letter After Drunken Junket Article Angers Military Leadership," *Ottawa Citizen*, June 11, 2019, https://ottawacitizen.com/news/national/defence-watch/20-dnd-staff-involved-in-writing-letter-after-article-on-drunken-junket-angers-leadership/. Accessed January 10, 2022.
[77] The prospects of that did not seem to bother Vance or other senior military leaders, who frequently appeared at events to raise money for military-related charities hosted by Taylor's publication, *Esprit de Corps*.
[78] UN Press Release ORG/1663, January 26, 2018.

military-media relations. Still, in certain DND quarters the view was: "PA had taken it to the media," and was applauded.

"What if the Pen is a Sword" (June 13, 2018)[79]

Later that spring, the Toronto-based Canadian Forces College published an otherwise routine staff paper, except this was by course attendee Janzen, soon to be promoted to (acting) brigadier-general and to be the new director general MilStratCom. The paper set out four points that offered new insight into the thinking behind the tweet storm and foreshadowed ideas that would mark the MilStratCom strategy.

First, the paper acknowledged the media's critical role in a democratic society but took umbrage with journalists in general and the Mali mission tweet brouhaha: "Senior CAF officers have faced disproportionate criticism in the past for minor public kerfuffles including … calling upon journalists to engage in deeper debates besides whether deployed military missions constitute 'combat.' These incidents were met with a barrage of outrage from select journalists." The paper argued that officers should have the liberty to highlight "adversarial information activity" and "disingenuous narratives," to encourage critical thinking [already a well-known practice]. Officers responding to "sensational reporting," it was argued, "may cause angst for a small minority of journalists with lower professional standards and ethics." This suggested an unhealthy adversarial relationship with media by Defence, the tenor and tone being that if as a mainstream media journalist or outlet you "did not agree (with) the Defence line," you were not just a critic, but a potential threat.

Second, the paper asked whether the CAF should influence Canadians and "generate desired effects among the population," this being answered in the affirmative. The officer made the case for Defence Public Affairs to shift from their traditional approach to inform audiences and adopt the concept of "ethical influence" to avoid being "drowned-out and possibly outmaneouvred by adversarial efforts." Communications to ethically influence domestic audiences needed to meet the suggested criteria of being "truthful, transparent and helpful."

While suggesting guardrails, including not to use deception techniques and taking care to not publicly influence policy and procurement, this proposal still raised eyebrows. Overt influence to generate effects sounded a lot like psychological operations.[80] "Ethical influence" as an operating principle for DND communications and for military Public Affairs doctrine, policy and practice would have serious consequences for organizational reputation and credibility. This is especially problematic applied in Canada if influencing behaviours, opinions and actions is the

[79] See https://www.cfc.forces.gc.ca/259/282/404/janzen.pdf. Accessed January 10, 2022.

[80] The CAF defines PSYOPS as "Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behavior, affecting the achievement of political and military objectives." From National Defence, DND and CAF Policy on Joint Information Operations, April 3, 2018, A3-3. In Canada and in NATO, PSYOPS is white, meaning the content produced is truthful and attributable, meeting two of the ethical influence criteria. A PSYOPS activity would only be done in the first place if authorities judged it to be helpful, meaning PSYOPS also matched the three ethical influence criteria proposed for PA.

communication's deliberate and overt intent, which implies more than just an effort to inform, educate or even to persuade.

A military influence campaign also prospectively unleashes the full range of resources and capabilities that a large department like DND can bring to bear to try to influence coverage, including through coercion. For instance, a journalist or media outlet whose coverage embarrassed Defence and/or affected senior military leaders could be internally regarded as a menace or even a threat to the institution and targeted for engagement with "non-kinetic munitions." This could include a concerted letter-writing campaign to the person's boss or outlet's owner, online trolling including from avatar accounts, whisper campaigns to other journalists, being denied interview opportunities, reduced access to officials or information, and trying to have the journalist removed from the Defence beat or fired.

At its core, ethical influence is an ambiguous framework with the potential for real abuse. The suggested guidelines of "truthful, transparent and helpful" are insufficient since these are relative concepts, usually defined by the creative talent or leader looking for desired effects in the information environment. "Truthful" – as determined by whom? "Transparent" – meaning a full reporting of all reasonably known facts and context, or merely acknowledging the source of the communication? And "helpful" – helpful to whom, as determined by whom?

Third, the paper introduced the idea for the CAF to consider "leveraging the skills of personnel from the IO community in domestic roles, but under Public Affairs doctrine and principles of ethical influence." This anticipated the later effort to introduce IO and PSYOPS staff positions into the Public Affairs group. Fourth was the underlying disdain for civilian practitioners and the lesser value of DND communications compared to an active military approach, arguing this was "far superior to bureaucratic, institutional communications which are faceless, distant and incapable of effective interaction and listening."[81]

Actions over the course of that spring to publicly condemn and marginalize media critical of Defence, along with a desire to expand IO's role into the domestic space, suggested to practitioners this was what "ethical influence" was about. "Commander's intent" was clear. The officer was promoted, became the senior military PAO and soon after received a significant military award for meritorious service. This signalled to the Public Affairs community that CAF leadership was satisfied with the approach and tactics. The MilStratCom initiative gained momentum and traction as more staff began to be freed up from their regular assignments to work full-time on the project.

[81] "What if the Pen is a Sword?," 24. The reality is considerably more nuanced. For instance, recent practice by now-former DND DM Jody Thomas, especially during the pandemic and in response to the Defence culture change file, stands as a notable if rare example of senior leader engagement with internal and external audiences that was public, personal and interactive.

Draft 'Concept' Papers Used as a Substitute for Approved Policy

The use of draft concept papers to progress work based on contentious policies without having to first obtain approval at the strategic level was a common practice at CJOC and the MilStratCom group in ADM(PA).[82] Four are of particular interest to our inquiry. These were no ordinary drafts (Fig. 3), having been prepared and professionally laid out in full colour with quality graphics, the Defence look and feel, copyright info and senior leader forewords, including attributions from Vance, Thomas, then-CJOC commander Lt.-Gen. Michael Rouleau and Special Forces commander Maj.-Gen. Peter Dawe. Many versions did not even include the word "draft" or a version number, and for all intents and purposes appeared genuinely issued and very convincing.[83] A number of other documents in development throughout 2019 in the MilStratCom group proceeded apace, driving work and showing the mindset at work at the time.[84]

This approach served multiple purposes. Slickly designed concept papers, especially if not marked "draft," about initiatives widely known to have senior military leader backing, gave cover and flexibility for staff to work as if the documents were agreed upon. It allowed the evolution of initiatives without the formality, delay and possible change or rejection by leaders, including the CDS, DM or minister, especially if cast as "operational level" documents not needing their approval, or without them even needing to be made aware. It helped when asking for new financial and personnel resources through the annual business plan since, for purposes of making the case, the policy changes seemed clearly on the cusp of being approved. As well, in sensitive spaces like policy, force development or information operations, any document that happened to circulate outside Defence and attract media attention could be dismissed as "just a draft, and not approved by leadership." This was also an effective way to avoid and/or delay ATI requests, believing that a draft document could not or would not be released.[85]

---

[82] A review in December 2020 directed by Vance determined that four concept papers, three of which were prepared at CJOC and one in ADM(PA), were key to influencing staff actions and "moulded staff mindsets about CAF and IO" (Maj.-Gen. Daniel Gosselin, Command Process Review – Canadian Joint Operations Command Information Operations Directives, December 28, 2020). (See ATIP A467694).
In June 2021, Eyre and Thomas concluded the concept documents were "championed by senior CAF leaders as surrogates for obsolete doctrine, yet they have lacked policy cover to ensure alignment with [government] intent and executive leader approval, and have thus been mistaken as authoritative." CDS/DM Directive – Response to Reviews of Information Operations and Influence Activities, June 9, 2021.

[83] The documents were so convincing that in January 2021, one of them (the Pan-Domain Force Employment Concept) was inadvertently posted on the Canadian Defence Academy website for a very brief period and tweeted about before being quickly pulled down.

[84] This included the June 7, 2019 draft Military Strategic Communications/Public Affairs Operationalisation Force Development Plan (with its acknowledgment that "Integrating a MilStratCom capability in the CAF may challenge the boundaries of current national policies…"); and the April 2019 draft CDS Directive for the Implementation of the Joint Information Operations and Military Strategic Communication Capability, which noted "MilStratCom and info ops force development is to occur simultaneously with force employment (**learn by doing**)" [bold added]. The information space with its consequences of error for institutional reputation and organizational credibility is not a field for untrained staff and inexperienced leaders to learn by doing.

[85] In fact, the act allows an exemption under Section 26 for a draft or parts thereof if the information will be published within 90 days of the request, though if a final report is not expected "in the foreseeable future … the drafts must be examined to determine if they can be disclosed or if other exemptions apply."

'How We Fight' (Feb. 10, 2019)

"How We Fight" (Figure 3-1), an artfully articulated think-piece by then-CJOC commander Rouleau, set in motion several developments and proposals for change in policy and doctrine to make the CAF more combat capable.[86] The *Strong, Secure, Engaged* defence policy nearly two years earlier had set out high-level tasks and established how much of each service would be needed to conduct different types of operations concurrently over defined periods of time. "How We Fight" was an effort to more fully explain the operational context and factors shaping conflict and inform upcoming senior-level discussions about what the CAF structure should look like.[87] The impact of the information environment on military operations figured prominently in the paper:

> "[The] CAF is operating today, every day, in the Grey Zone. We are in conflict with nation states below the threshold, largely in the informational space which is fast becoming the CENTRAL theater for strategic competition. We see this In Ops REASSURANCE and PROJECTION most especially…"[88]

Rouleau, who spent most of his military career in Special Forces, was a high-profile and energetic advocate for a more strategic approach by the DND/CAF to operational and institutional communications. This provided a real impetus for more rigorous information operations-related contributions to the work of the CJOC HQ, including a staff re-organization that assigned an army combat arms colonel as information component commander to head a substantially sized joint operations effects cell. [89] "How We Fight" was instrumental in energizing the production of a number of draft support concept policy documents and draft directives to evolve the forces and capabilities needed "to compete with, contest, confront, and – when necessary – combat our nation's adversaries…"[90]

The CJOC was very good at managing the deployment of forces overseas for a variety of missions and demonstrated real aplomb at organizing efforts throughout the country to support long-term health-care facilities, help deliver vaccines country-wide and assist communities to deal with floods and fires. The explicit focus on combat and below-the-threshold-of-conflict of "How We Fight" and the concept documents it spawned, though, left no room for complementary "when we

[86] Lt.-Gen. Michael Rouleau, "How We Fight," Commander CJOC's Thoughts, February 10, 2019. The initiative was a CDS-supported undertaking on behalf of the CAF.
[87] In July 2020, Rouleau changed jobs, from commanding CJOC to be vice-chief of the defence staff (VCDS). In March 2021, it was announced Rouleau would become a strategic advisor to the CDS with a focus on improving the interoperability of military combat capabilities, making room for Lt.-Gen. Frances Allen to be VCDS, the seventh person in four years to hold the position. That June, Rouleau announced he was stepping aside to leave the CAF in the face of criticism for a public outing with the RCN commander and former CDS Vance who was still under military police investigation. See Amanda Connolly, "Canadian Military's Second-in-Command Resigns Role After Golfing with Vance," Global News, June 14, 2021, https://globalnews.ca/news/7948266/canadian-forces-mike-rouleau-golfing-vance/.
[88] Op Reassurance refers to CAF deployments in Central and Eastern Europe as part of NATO's collective defence; Op Projection refers to frigate deployments worldwide.
[89] Lt.-Gen. Michael Rouleau in, "Manoeuvre in the Information Domain," *Canadian Army*, May 4, 2020. The experiment with the Joint Operations Effects-named cell turned out to be short-lived.
[90] These included the Pan-Domain Force Employment Concept (PFEC); the Joint Information Operations Force Employment Concept (JIOFEC); the Military PA Enhancement and Employment Concept (MPAEEC); CDS Guidance on Military Strategic Planning; and, by MilStratCom in ADM(PA), the CDS Directive for the Implementation of Joint IO/MilStratCom, and the MilStratCom/PA Operationalisation Force Development Plan. All these documents proceeded to substantive draft form, but none obtained approval.

are not fighting" type of direction and guidance for domestic operations, though requests for CAF support at home had increased multi-fold over time.

The Pan-Domain Force Employment Concept (PFEC) (Spring 2019)

"How We Fight" led to the development of three notable operational concept papers. The draft "Pan-Domain Force Employment Concept" (PFEC, Fig. 3-2) was intended as the overarching blueprint to shift thinking at Defence, "first and foremost, to initiate immediate changes to CAF force employment … a driver of change starting today,"[91] making the case it was neither strategy nor policy. Since the PFEC was a conceptual foundation "for how the CAF must fight," and was "designed to put us on a war-footing to reflect the immediacy and urgency of the threat,"[92] the initiative suggested a major evolution of policy and not a natural extension and tweak to *Strong, Secure, Engaged*. As Brig.-Gen. David Anderson, CJOC chief of staff readiness, explained, "The last thing we want to do is to prepare to fight the war we want as opposed to the war we have, and the war I believe we are now in."[93]

No one at Defence disputed the urgent need for change to improve the CAF's ability to fight and win in contested campaigns, but the adage that "if the only tool you have is a hammer, you tend to see every problem as a nail," seemed applicable. That is, preparing for major conflict overseas against malign state actors and terrorists permeated policy development work. That work needed to be done, of course, but crowded out discussion about how to improve capacity and capability to better support civil authorities for tasks that formed the vast majority of the CAF's operational activities, including fighting fires, floods, SAR or even helping feed or take care of patients at long-term care homes during a pandemic. It also coloured all the language used: even in routine settings at home, Canadians were considered "targets" to be "engaged" with "non-munitions capabilities," in order to be "influenced" using "information operations." Incredibly, many staff and senior leaders were oblivious to how this would be perceived by media, DND/CAF partners, politicians and the general public.

The Joint Information Operations Force Employment Concept (JIOFEC) (Spring 2019 – 2021)

Of the various proposals prepared during the MilStratCom initiative, this document stands out for the degree of disconnect of the operator and IO communities from the norms of military-civilian relations. The JIOFEC (Fig. 3-3) was initially intended to be an annex to the PFEC, but challenges of securing approval for the latter led staff to plan to issue the JIOFEC separately as a primer. At the end of June 2020 as the pandemic raged, significant internal angst about IO had

[91] PFEC, 8.
[92] National Defence/Canadian Joint Operations Command, PFEC, 4, and CJOC briefing, "How We Fight," October 3, 2019.
[93] Canadian Global Affairs Institute, Defence Deconstructed Podcast, "How Canada Fights," August 28, 2020. See https://www.cgai.ca/how_canada_fights. Accessed January 10, 2022.

been building at NDHQ and in the end, the JIOFEC was not signed.[94] That such a document could come so close to approval by very senior officers illustrates the failure of governance and oversight in the MilStratCom initiative.[95]

The JIOFEC was intended to "shape how we train, equip, structure, and fight in the information domain," and like the PFEC, was new policy but not acknowledged as such: it was thought that concepts only needed the operational HQ's (CJOC) approval. The document set out several elements of the problem statement that would be hard to argue against, including that the "CAF has a mindset issue" about operations in the information environment; there was no champion for the conduct of IO; the military did "little to systematically take purposeful, joint and coordinated action" in the information environment; and there was little consideration for joint employment of information-related capabilities.

The document explained that the CAF had not developed any comfort in delegating authorities to conduct IO outside of conflict, which was true enough and as events would prove, for good reason. It was argued the situation "imposes restraints" on IO's ability to "protect and promote Canadian interests and equities." The proposed answer to that dilemma was the JIOFEC, which "will allow us to shift from a responsive posture to an anticipatory posture vis-à-vis policy, authorities, mandates and capabilities" across the breadth of CAF pan-domain operations – an astonishing and likely illegal practice.

With timely direction and agreement from the government and armed with these anticipatory authorities, it was thought the CAF could then develop IO solutions in support of "Government narratives and initiatives," and help with "shaping the information environment for future military operations." The drafters also set out that the CAF needed to change how military members, decision-makers, allies and partners view targets and to remove "ambiguities such as munitions targets, non-munition targets, cyber targets, etc." because "There exists only targets."[96] It was all so very stark – "our processes and structures are no longer effective at offering responses to modern operational problems" – with the overt idea being that leaders (at least, those outside of CJOC) were blind to the possibilities the IO toolkit could provide, if only the staff could be unleashed.

[94] The JIOFEC continued to evolve under Lt.-Gen. Christopher Coates, who replaced Rouleau as commander CJOC in summer 2020. Even after the document's deficiencies had been acknowledged in formal reviews, efforts continued to produce a concept that, "pending approval, will define the CAF's functional approach to compete with, contest, confront and when necessary, combat our nation's adversaries in the information domain." (DND Departmental Plan 2021-2022, 13). The last version of the CJOC effort noted that, "While Joint Information Operations remains an integral part of expeditionary operations, the use of Joint Information Operations within the Canadian domestic context is currently restricted, with the sole exception being in defence of North America. For the purposes of Domestic Operations, the employment of Joint Information Operations is strictly prohibited unless otherwise superceded by a CDS Directive. This, however, does not preclude the use of specific [information-related capabilities] in support of Government of Canada initiatives during Domestic Operations or other Domestic initiatives." (See ATIP A-0503623, 15). This torturous description trying to provide policy guidance on how activities, some invasive and coercive, could simultaneously be prohibited and allowed neatly illustrates the confusion that reigned.

[95] As CJOC PAO Capt. Gregory Cutten explained, "There will be no further progression of this document. Although CJOC continued to refine the document at the working level during 2020 and 2021, it was determined that the draft document was obsolete with respect to the evolving information environment and the [CDS/DM Reset Guidance of November 2020]." Email communication with author, April 8, 2022.

[96] JIOFEC, 19.

The Military Public Affairs Enhancement and Employment Concept (MPAEEC)[97] (Spring 2019 – November 2020)

The MPAEEC (Figure 3-4) was the third key draft concept document offshoot of "How We Fight" and its title marked an important shift in the lexicon being used. Notably, in mid-June 2020, the director general MilStratCom had quietly changed job titles and the initiative name to Military Public Affairs, in acknowledgment that the MilStratCom term was weighing down the overall effort.[98] The MPAEEC referred to the JIOFEC no fewer than five times, describing that document as the framework to shape how PA would be organized and employed; it also explained that efforts would be aligned with a Defence StratCom concept being developed by the strategic joint staff (another concept, the fourth, by yet another group), aiming "to influence the attitudes, beliefs and behaviours of audiences," including domestically.

As explained in Chapter II, the MPAEEC described five key deficiencies of Public Affairs and detailed 22 initiatives to improve capability, nearly all being unquestionably useful and needed, such as enhancing visual communication, updating policies and doctrine and improving the co-ordination of communication campaigns.[99] This was a widely welcomed effort to enhance capability that had grown less effective. However, the narrative framing of the need and effort was jaundiced. Although CAF PA practitioners were "widely recognized for their expertise" and DND communications "lauded as among the best in government," nonetheless, the concept paper was severely critical of the function, claiming that it "lacks the proper readiness to effectively support overseas operations."[100] This indictment would come as a great surprise to the hundreds of PAOs over the years who had deployed on several dozen expeditionary operations and missions of all kinds and served with recognized distinction in multiple Canadian, U.S., U.K., NATO, allied and coalition headquarters in war, conflict and peace – thereby earning for PA the reputation earlier lauded.

The hyperbole of the concept paper appeared crafted to ingratiate the reform initiative with hard-core operators, but the overall characterization of PA incompetence simply reinforced a built-in propensity by those already inclined to dislike the function. Putting the burden of responsibility for the situation on Public Affairs absolved senior leadership of responsibility to actively engage – since the problem set was, by the branch leaders' own explanation, fundamentally an issue of

[97] National Defence, Military Public Affairs Enhancement and Employment Concept, draft 9.2, October 2020 (See ATIP A0527354). The original formulation of this concept was the CAF Military Strategic Communications and Public Affairs Operationalisation Force Development Plan (See ATIP A0527355).
[98] The MilStratCom concept continued to take fire from media and generate concern among some serving PAOs and other practitioners; thus, internally the term was dropped, though it continued to feature prominently on the initiative lead's social media accounts and in briefings to external audiences. The title change was acknowledgment that the lexicon had contributed to a stall of overall momentum and perhaps could lessen the risk of blame for public missteps by non-PA information-related capabilities, mainly IO and PSYOPS. The "Military Public Affairs" designation stayed until November 2020 with the cancellation of the MilStratCom/MilPA initiative, and the job title reverted back to director general Public Affairs, a longstanding convention.
[99] The three of dubious value were: support implementation of the JIOFEC, create a distinct military PA unit within ADM(PA) and establish a social media task force separate from the existing capability in ADM(PA).
[100] "Currently the wider CAF does not adequately understand the information environment, does not have the expertise required to act effectively, is not properly coordinating activities and information across the enterprise, and has little ability to determine if actions are achieving strategic effect," concluding that "this results in ineffectual engagement in the military information domain and global information environment." MPAEEC, 9.

the PA group's own training and skill level, not a consequence of outdated policy and institutional design. The effort to minimize members' previous service and claim that deployable PA capability was a new idea also rankled serving and retired PAOs who remained close to ongoing developments or were employed in the function elsewhere. Still, the prospect of a vision, any vision, along with new training, deployment opportunities, capability investments and career prospects was enticing and led to broad military PA support.

The effort by MilStratCom's leads to separate institutional communications and operational military communications into distinct groups, even if operating "in close coordination,"[101] created two notable fissures. First, was the view that institutional-thinking civilian practitioners were less valued than their military counterparts: civilian staff laboured on "recruiting and other benign institutional priorities," and did not deploy in direct support of active operations outside Canada. PAOs and imagery technicians were encouraged to consider themselves as "central to the information fight" and "information warriors," or otherwise were "corporate PR agents."

Second, this effort at separation drew significant financial and personnel resources from the Public Affairs functional authority, undercutting that group's own joint DND/CAF PA transformation effort taking place at the same time. By summer 2020, the MilStratCom/MilPA initiative had grown to be the single largest funded group within the Public Affairs group – excluding only the section that bought recruit advertising – drawing away the senior most PAO (one brigadier-general), and the senior PAO colonel (of just two at that rank).

In large measure, the MilPA team had simply unplugged itself from active Public Affairs support, except for a short period in spring/summer 2020 during the pandemic when all hands absolutely needed to be on deck.[102] Over a period of about two years, this approach weakened Defence's overall ability to more effectively support the relentless ongoing operational demands, advise institutional and military leaders, conduct strategic planning and to proactively build information campaigns and content to explain Defence activities to Canadians – the principal function of Public Affairs (Fig. 4).

[101] Ibid., 7.
[102] The pandemic provided an opportunity for the team to trial different products from a military PA perspective, to try to demonstrate perceived shortcomings in the institutional ADM(PA) effort but served instead to highlight inherent biases. For instance, a draft COVID-19 heat-map information environment assessment (Figure 5-2) designed to help brief commanders chose "hostile" through "permissive" as labels to describe a variety of criteria, including how media were reporting about the military. This language choice illustrated the problem of approaching every need through the lens of contested operations and showed how the group viewed mainstream media. The continual effort to try to establish a new and distinctly military capability to justify the initiative and resource spend, rather than help to improve existing services and products prepared by ADM(PA) staff on a regular and often daily basis, duplicated effort and drained staff time and energy at a time of great need for both.

The MilStratCom/Mil PA Ethical Framework (Summer 2019 – Fall 2020)[103]

By early summer 2019, it was clear that progress on the various information-related capability initiatives had lost momentum, except for some upgrades in PA training and improvements in the imagery technician trade, who now all worked for Public Affairs.[104] Other efforts continued apace, including trying to secure support for the concept papers but traction was intermittent, and it was increasingly a struggle to explain the initiative to parties inside and outside Defence. Work on the Joint IO/MilStratCom force development plans had been quietly shelved and replaced by a new iteration, renamed the MPAEEC. A number of practitioners were concerned with what they were seeing and hearing being prepared, including force generation strategies for IO and PSYOPS being developed by Public Affairs staff; an authority chart setting out the use of military deception against Canadians and allies; incorporating IO and PSYOPS in the PA organization chart; a "learn by doing" approach in the informational space; and the MilStratCom group mantra that "the motto 'who dares, wins' is applicable to strategic communication as it is to warfare."

More than just verbal assurance was needed to convince staff that elements of PSYOPS and military deception would not creep into Public Affairs work, especially within Canada. Thus began an extended effort to try to codify an ethical framework to provide guidance to and enhance ethical decision-making by practitioners. In essence, a code of conduct was proposed. This muddled effort to set ethical boundaries illustrated the challenge and practical dilemmas still resonating within the affected communities about how best to articulate concepts of targeting and influencing audiences, especially in Canada.

After one-on-one consultations in 2019, this MilStratCom product evolved over the next 18 months, seeking to address anticipated or perceived criticism of the overall initiative. Consistent with titles for individuals, the framework's name shifted from MilStratCom to MilPA (Military Public Affairs), revealing that at its core, this was still an IO/MilStratCom effort. The exclusive focus just on military PA practitioner behaviour missed an opportunity to articulate ethical boundaries and considerations for commanders and staff. The framework also excluded civilian practitioners, who in fact represented the majority of the PA practitioner community at DND and also actively supported operations. The notion again, that military PA had a separate and unique role to play as a communications enabler challenged and undercut the functional authority for Defence Public Affairs, a position assigned to a civilian assistant deputy minister.

While the framework emphasized longstanding PA touchstones like truthfulness, transparency and attribution,[105] the language wandered well outside the bounds of federal and defence

[103] The author is grateful to retired PAO Capt. (N) David Scanlon for discussions and feedback about the MilStratCom/MilPA ethics framework. (Document, see ATIP A0527353).
[104] Notably, this included new courses in social media for operations (one week) and for StratCom enablers (one week); attendance on operational targeting for military PAOs and operational planning; attendance at joint command staff course and the national security program; and work on a new actor and audience analysis course of seven weeks – a course that would end up in the news in October 2020.
[105] As far back as 2007, NATO's Military Committee agreed on new principles of NATO military PA, including and especially for deployed operations: tell and show the NATO story; provide accurate information in a timely manner; ensure the information provided is consistent, complementary and co-ordinated; practise appropriate operational security; and conduct work mindful of multinational sensitivities and respectful of the local and regional cultural environment. See Brett Boudreau, "Readier for a Brave New (Wired) World: Highlights of the New NATO Military Public Affairs Policy," *The Three Swords* (NATO Joint Warfare Command), December 2007, 25-30.

communications policies. To bracket its more controversial elements, the framework suggested a new principle of "civil control of domestic persuasion." The proposal was that persuasion would be limited "only to the point where citizens consider and understand the military viewpoint on appropriate issues," with such efforts stopped at this "point of enhanced understanding." This formulation with its vague and subjective threshold revived the earlier concept of "helpful" ethical influence and offered little practical guidelines for practitioners. The framework also noted that "any collection of data on citizens must have prior government approval," suggesting something more than simply analyzing the information environment, developing assessments and observing and discerning trends, one of which required data collection on Canadians.

In the end, the effort did not sufficiently convince stakeholders of a need for a separate and additional ethical framework unique to communicators. Service members in many other military disciplines faced equally or even more demanding circumstances in their work and moreover, along with their civilian colleagues all are guided by the DND/CAF Code of Values and Ethics.[106] Unquestionably, there is real value in exploring how each unique discipline should apply that code, especially in a fast-changing domain like information, but the proposed framework strained to define new and questionable practices as ethical. Rather than advancing other key work to progress revised PA policy and doctrine, the undue effort to try to detail additional ethical principles, values and expected behaviours created further suspicion about the overall initiative. At best, the ethical framework was an earnest effort to square a tough circle but was not approved, another casualty of the approach to limit outside engagement in support of the development of related policy and product.

For the prospective information warrior though, the stage was now well and truly set. There was overarching Defence policy cover through *Strong, Secure, Engaged* to develop an offensive information operations capability during conflict but especially in the so-called grey zone. The CDS/DM Joint IO Policy afforded wide freedom and latitude to operational headquarters to engage in the informational space. Initiative leads could and did play "the CDS said he wants it this way" card. The reserve force in the army had been tasked to generate people to do the work and improve the capability. There was now a high-ranking operator willing to openly champion the initiative – one widely expected to be the next vice-chief of the defence staff and a contender for CDS. The CJOC had been empowered to lead IO policy and capability development, informed by an approach that considered everyone a target, and the country in undeclared war. A full-time MilStratCom team in ADM(PA) worked to expand PA's role into the influence realm.

The trouble was that the collective Canadian military leadership had never been serious about developing an enterprise-wide foundation for the competent use of such capabilities. The policies, doctrine, training, structures, governance mechanisms and force development work, let alone appropriate oversight or unbiased external advice to help navigate prospective pitfalls, were not in place. The CAF knew about and documented these shortcomings. Except for PA, the information-related capabilities lacked just about every quality needed to lend the effort any

[106] See https://www.canada.ca/content/dam/dnd-mdn/documents/reports/code-value-ethic-en.pdf. Accessed January 10, 2022.

reasonable chance of success including jointness: the navy and air force wanted nothing to do with it and the army owned it all but acted as if it wanted nothing to do with it.

This situation should have informed a top-down, deliberate, structured approach to policy and capability development, including early, written, senior-level direction. Instead, initiative leads were allowed to forge their own independent and parochial paths, coming together with colleagues from other lines of effort infrequently and only if absolutely required. Stakeholder engagement inside and outside Defence was regarded as a burdensome obligation, not a prospective benefit. As one senior officer described his experience, "rather than seeing others as collaborators, we were seen as critics and naysayers to be outwitted with nuanced language and declarative ethical frameworks. If a collaborative approach had been taken, the initiative would have been light years ahead."[107]

By late fall 2019, it was clear the elements still operated in a disconnected fashion, and that the MilStratCom initiative with its constituent parts working independently was not delivering the goods. Consequently, the CDS directed the strategic joint staff to pull together a StratCom working group to develop options for senior leader consideration, of how to organize the capabilities to take work forward faster. The working group, with representation from nearly two dozen entities and offices across the DND/CAF, began its work in mid-December. Though the MilStratCom initiative was more than four years old by then, this was the first time for a co-ordinated effort among the many affected offices to share information and work toward a joint solution. Early in 2020 though, the pandemic took hold and staff were drawn to other pressing assignments. And in April 2021, CJOC issued an IO annex for the pandemic response, triggering a brand-new chapter in the saga.

[107] Interview with senior PA practitioner, January 2022.

IV: The Initiative Runs Into Heavy Turbulence

Restricting the Release of Unclassified Information

There were at least a half-dozen obvious warning signs in Canadian media coverage in the latter half of 2020 to suggest something seriously amiss in DND communications policy, processes and management, signals that leaders and practitioners missed or ignored. The first overt indication was a June 8 story of the initiative – ironically, leaked to the media – to limit the number of leaks and inadvertent or unauthorized releases of unclassified information from DND.[108] The intent of the "safeguarding information" administrative order was to create a "for official use only" designation like that used in the U.S., permitting the release of non-classified information only to authorized parties. In large measure, the impetus to develop the policy stemmed from a seemingly non-stop litany of leaks resulting in multiple media articles on a variety of issues – made worse by bungled public affairs – that regularly embarrassed Defence and senior military leadership.[109]

The policy, widely staffed and on the cusp of being issued against the advice of civilian Public Affairs officials, sought to subject all unclassified information at Defence to review before release by an "appropriate authority." Consistent with the process for classified material, the release authority would normally be the office or person who created the record. Under the proposed policy, the responsible office or person would have been required to consider the information's sensitivity level, the requestor's security level and proof of the requestor's demonstrated need to know to determine if the information could be released. The draft policy also specified that "suspected non compliance" with the instruction "may be investigated" with possible offences reported to "responsible law enforcement agencies," which was an intimidating proposition.[110]

Though approved by senior management, the approach should have been identified early on as both unwise policy and administratively unfeasible. The sheer impracticality of the proposed stricture and considerable staff cost to assess each document created, monitoring where the

[108] See David Pugliese, "Canadian Military to Crack Down on Leaks of Unclassified Information After Recent Embarrassments to Government," *Ottawa Citizen*, June 8, 2020, https://ottawacitizen.com/news/national/defence-watch/canadian-military-to-crack-down-on-leaks-of-unclassified-information-after-recent-embarrassments-to-government/wcm/9abe70d9-5bd7-4cf4-8cfd-34fead874304/. Accessed January 1, 2022.

[109] A lack of openness and transparency on Defence's part contributed to the recurring problem of leaks, with stories made more damaging because of an unusually confrontational approach at the time by Public Affairs leaders with media critical of the military, which strained relations and affected coverage of Defence. Knowledgeable serving personnel were taking issue with official lines offered by spokespersons about missteps and continued to contact media, leading to more articles. Figure 1-1 is an example of the Public Affairs reaction to media coverage of the incident, illustrating a strategy of obfuscation that helped generate critical media stories for months. See David Pugliese, "Canadian Forces Misled Media and Public on Taxpayer-funded VIP Booze Flight," *Ottawa Citizen*, Nov. 5, 2018, https://ottawacitizen.com/news/national/defence-watch/canadian-forces-misled-media-and-public-on-337000-taxpayer-funded-vip-booze-flight. Accessed January 1, 2022.
Another story that fuelled internal demand for a release-of-information directive stemmed from concerns about information leaks following the April 29, 2020 crash of an RCAF Cyclone helicopter (Stalker 22) in the Ionian Sea. The initial Defence/CJOC communications about the incident (Fig. 4-2): "Contact was lost with the aircraft as it was participating in Allied exercises off the coast of Greece … Search and rescue efforts are currently underway…" gave the impression the platform was lost at sea in an unknown location. Through tips, days later the media revealed important information about the crash, including that the helicopter went down within sight of the ship's crew. Several media criticized the incident as a deliberate attempt by Defence to mislead the public and referenced by some as a (bad) example of influence operations. See Scott Taylor, "Source of Misinformation Released After Cyclone Helicopter Crash Not Revealed," Saltwire, July 5, 2021, https://www.saltwire.com/atlantic-canada/opinion/scott-taylor-source-of-misinformation-released-after-cyclone-helicopter-crash-not-revealed-100608089/. Accessed January 1, 2022.

[110] DAOD 2006-1, final draft March 2020.

information might be made available and trying to enforce compliance would have cost millions of dollars in staff time. The policy's language about the need for strict compliance to prevent injury and "the impairment of the proper functioning of government institutions" bordered on the disingenuous since trial balloons and discussions by political staff and senior military and civilian officials with persons outside the DND/CAF are a necessary part of public administration: of course, the policy wasn't meant to be applied to those "knowledgeable parties," but to those who shared information that embarrassed the department in the media.

The policy would have set further, serious limits on the disclosure of even mundane information from National Defence for nearly any purpose. Treating unclassified information as "secret unless proven otherwise" rather than "open unless proven otherwise" would have hampered DND's ability to conduct any activity. Vance told the policy leads to start over and a substantially revised version with the same general intent was issued 18 months later in January 2022.[111] It would not be the first time that media coverage exposing embarrassing activities coming from leaks by concerned parties within Defence would force senior leaders to reconsider MilStratCom-related activities in development or already underway.

The Information Operations Annex for OP LASER: CAF's Response to the Pandemic (April 8, 2020)

In July 2020, soldiers from Joint Task Force Central HQ in Toronto contacted the same Postmedia reporter, David Pugliese, who broke the disclosure-of-information story. The soldiers expressed concern about the legality of being tasked to collect information on Canadians from social media accounts during OP LASER – the military's effort to help civil authorities fight the pandemic, including assisting at long-term care facilities.[112] A group called the precision information targeting team had been formed from the army's influence activity unit, tasked to support and report to the intelligence section. Activities consisted of social media monitoring, outreach with key provincial, municipal and military stakeholders and PSYOPS staff preparing information material as well as amplifying work by other government departments.[113]

---

[111] On January 12, 2022, a notably revised version with improvements having the same original intent was issued. The DND/CAF now has a formal instrument to more clearly control the release of unclassified information and for prospective sanction of those who release information inadvertently or intentionally. This bears watching to learn if the administrative order improves or constrains the public release of information by Defence that has not been classified. See Department of National Defence, Defence Administrative Order and Directive 2006-1 Procedures for the Safeguarding and Authorized Disclosure of Information in the DND and the CAF, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-1-procedures-safeguarding-authorized-disclosure-information.html. Accessed March 15, 2022.

[112] See David Pugliese, "Canadian Forces Information Operations Pandemic Campaign Squashed After Details Revealed to Top General," Ottawa Citizen, July 20, 2020, https://ottawacitizen.com/news/national/defence-watch/canadian-forces-information-operations-pandemic-campaign-squashed-after-details-revealed-to-top-general.
Accessed January 2, 2022.

[113] Later, through ATI requests, it was revealed that one of the team's areas of interest was the Black Lives Matter movement, a development that Trudeau called "worrisome." See David Pugliese, "Canadian Military Intelligence Monitored Black Lives Matter Movement Claiming Pandemic Justified Such Actions," *Ottawa Citizen*, May 11, 2021, https://ottawacitizen.com/news/national/defence-watch/canadian-military-intelligence-monitored-black-lives-matter-movement-claiming-pandemic-justified-such-actions. Accessed January 2, 2022.

The article revealed that nearly three months earlier, the Canadian Joint Operations Command (CJOC) HQ in Ottawa, in charge of all domestic or overseas military operations, had released an Information Operations (IO) annex to subordinate units throughout Canada. The story included worrying insight into the mindset that informed CJOC's approach to information operations. Then-chief of staff Rear Adm. Brian Santarpia explained to the reporter that in his view, there was no requirement to check such orders with senior headquarters ahead of release and, "The young folks we have that are keen on this sort of understanding the information sphere and then using these sorts of tools … we don't restrain that sort of initiative." These comments in print, even after the internal brouhaha when the IO annex was issued, offered two giant red flags – that the CJOC considered they had a prerogative to conduct IO on their terms without approval since IO was an "operational level" remit; and that staff and practitioners qualified or otherwise would be "learning by doing" without appropriate oversight. The article rekindled a long-simmering debate in Defence about the role, place, authorities and oversight of such activities, especially in a domestic context, but did not result in explicit action to change course.

Some backstory: in mid-April 2020, senior Public Affairs practitioners learned that CJOC intended to issue an IO annex for the pandemic support operation named LASER, and conscious of the potential short- and long-term reputational repercussions, alerted leaders at National Defence Headquarters. By then, though, the document had already been issued days before by CJOC, without having been sent for review outside the headquarters. This generated considerable discussion and exchanges among strategic staffs.

In the early days of the COVID-19 pandemic, planners could only guess at how the virus would impact Canadian society, and the scale and scope of prospective CAF support to civilian authorities. Staff needed to consider a number of what-if worst-case possibilities, including how to respond in the event of wholesale infection in First Nations communities across the country; major outbreaks in prisons incapacitating guards and affecting the inmate population, leading to riots; widespread civil unrest including looting; or a combination. Overseas operations needed to be sustained and forces rotated all while following new, stringent force-protection measures. There was always the possibility a malign actor would use the distraction of the pandemic to cause trouble overseas. And there was no way of knowing the impact of COVID on DND/CAF members and the institution's ability to generate healthy troops for operations.

The CJOC HQ did an admirable job juggling all those balls. At the same time, the pandemic was viewed as a unique opportunity to "grow and define the relationship between Canadians and their military," to practise in a domestic context the new capabilities under development and to test assumed authorities under the approved Joint Info Ops Policy. As Santarpia explained at the time, "This is really a learning opportunity for all of us and a chance to start getting information operations into our [CAF-DND] routine."[114] The responsible section head, Col. Chris Henderson, told the head of a fact-finding review he was excited to have an opportunity to experiment with translating IO doctrinal concepts for domestic operations.[115] The IO annex objectives for the

[114] Gosselin, Command Process Review – CJOC Information Operations Directives, 20.
[115] Ibid.

military were that Canadians are "deterred from participating in Civil Disobedience," "civil order is maintained" and the public's "compliance with suppression measures is reinforced." Ominously, the document described a threat as "any real or potential condition that can … lead to mission degradation."[116]

The document read like it was borrowed from a standard template for the Afghanistan mission, with a call to "conduct village assessments," engage religious leaders as a key audience and be prepared to deploy vehicle-mounted loudspeakers and portable radio stations.[117] Subordinate units were tasked to support government and civil authorities to proactively mitigate the effects of mis- and disinformation "*regardless of their provenance or intent*" (italics added) – an unfeasible undertaking, and not requested of the military. It also directed that "PSYOPS and other [information-related capabilities] will be leveraged in support as enabling capabilities to enhance PA and OGDA [other government department and agencies] communications." In other words, assets meant for contested overseas operations were put on call for use in Canada. As national security expert Wesley Wark explained, "The military analogy being drawn on was, in effect, an artillery or aerial bombardment, but with the exception that information operations were not constrained to activities against a known adversary. The public was the bombardment target."[118]

At the same time, for the same operation, in addition to the IO annex, CJOC was also busy issuing a Strategic Communications annex and a Public Affairs annex, with subordinate and superior headquarters issuing other instructions in the same vein – the result being a cacophony of guidance, direction and messaging at odds with the MilStratCom intent of synchronizing the effort.

After learning the IO annex had been issued, Vance immediately ordered it rescinded. The incident also earned a rebuke from Sajjan, who ordered a review into the intelligence collection activities, the first of four formal investigations into MilStratCom-related missteps over the course of the year.[119] Still, it was three months later and only after more negative media coverage that in early July, Vance verbally directed that henceforth, "the CAF will not conduct Info Ops during domestic operations or directed against domestic audiences, except when authorized for the defence of Canada against an armed adversary."[120] The circumstances around how the IO annex was issued and the subsequent frank discussions within the CAF were the first open illustration

[116] Canadian Joint Operations Command HQ, Annex UU to 3350-OP LASER OPERATIONS ORDER 002, 08 APR 2020. (See ATIP A2020-00660).
[117] A subsequent Canadian army investigation into the PSYOPS capability determined that the radios-in-a-box (RIAB), useful in settings such as a counter-insurgency operation with a need to broadcast to an isolated village or town, could not be used in Canada because there were no radio licences to operate them, as required by law. Canadian Army Doctrine and Training Centre, Review of Influence Activities Function Within the Canadian Army, January 27, 2021. (See ATIP A0525769).
[118] Wesley Wark, "The Pen and the Sword: Information Operations and the Domestic Environment," (report for Defence Research and Development), March 2022, 26.
[119] Formal investigations and reviews were launched into intelligence gathering during OP LASER, a September 2020 PSYOPS exercise in Nova Scotia, the Canadian army's influence activity capability, and in December 2020, the release of the IO annex by CJOC HQ.
[120] Interview with attendee at CDS Operations meeting, July 7, 2020. It does not appear that the CDS direction was issued in writing under his signature but was "well enough understood by all" and put everyone on notice that IO, but for the wrong reasons, had finally got the attention of senior leaders. The November 2020 Guidance and June 2021 Response to Reviews Directive discussed earlier, both offered further, if not complete clarification, noting the new intent of "ensuring that no domestic military operations in the [information environment] are directed at Canadian citizens." (Directive, 1).

internally of the depth of disconnect that had been brewing for years between operational planners and the strategic headquarters, the consequences of seriously outdated doctrine and the institution's inability to appropriately provide effective oversight by the designated authority, the Strategic Joint Staff.[121]

The Army Seeks to Influence Decision Management Boards at Defence

In August 2020, a highly unusual post appeared on the government's "Buy and Sell" online portal. The Canadian army's deputy commander was looking for a contractor to help address the army's "difficulty in communicating its cost of business, particularly from an equipment support perspective at the departmental senior governance level."[122] The statement of work noted the army "struggles" with explaining the costs of its activities compared to the navy and air force and that had "significantly impacted the [Canadian army] in terms of funding allocations throughout the years…" The document identified four internal senior management groups to target initially and also asked the winning contractor for "no less than 2 distinct key narratives that would resonate outside the [army]."

The request for services suggested major internal governance and process problems at DND/CAF in the quest to develop a balanced mix of big-ticket military capabilities. The call for support was also a serious indictment by the army of its own leadership over many years and the institution's Public Affairs function. If even the senior-most decision-makers at Defence were insufficiently informed about the role, place and requirements of the army to decide on billions in budget allocations, then that did not bode well for general awareness of that service's raison d'être with the broader Canadian public. The proposal set out very specific and narrow mandatory experience requirements for the prospective contractor, suggesting a fix was in for a particular person. As it turned out, no qualified bidder was found and the initiative was also quietly shelved. Coming soon after the IO annex debacle, the incident added to growing concern inside Defence about the prospective use of overt influence tools and techniques to obtain desired military outcomes, not just in Canada, but among and against the institution itself.

The "Fake Wolves" Exercise

In early October 2020, media reported on a PSYOPS reserve army training exercise in Nova Scotia the month before that had gone wrong. The exercise was meant to practise how to develop and

[121] The Joint IO Policy (2018) assigned functional responsibility for CAF information operations to the Strategic Joint Staff's head, the director of staff (DOS).
[122] https://buyandsell.gc.ca/procurement-data/tender-notice/PW-20-00922396?source=email__;!!O9lNpA!1GBbdWsi1JXIIHrYO3y8J5NRtCnZe8hClfBE3r1hjXu7Eic3qNKSkeieW74PA9I4$. Accessed January 10, 2022. This was the subject of one media story, but in Blacklock's Reporter, an Ottawa-based internet publication with a high subscription price, which limited broader media attention.

execute an influence campaign, something practitioners would expect to do in real life on overseas operations against malign state and non-state actors. Rather than test such a scenario, staff created a fake letter purportedly from provincial officials warning that grey wolves had been introduced into the area, were on the loose and posed a danger.[123] A realistic touch to the training was the use of loudspeakers blaring wolf sounds in the exercise area.

A copy of the fake letter was found in the location where troops were training. Without markings identifying it was for exercise purposes, a concerned soldier thought it was real, took a photo and sent it to his spouse, who shared it with friends. The letter began to be more widely distributed online, leading to calls to local officials who were forced to publicly dismiss the false claim through the media and question whomever could be behind the ruse. The unit quickly fessed up and a military investigation was launched: early findings then also led the army to order a broader examination of the entire influence activity capability. The comical story was picked up widely in media across Canada and internationally including the *New York Times*, *Vice* and *Russia Today*, the Kremlin-sponsored propaganda outlet, which set the incident within the broader array of military strategic communications issues and missteps reported on in Canada over the year.[124]

Defence Public Affairs Spends $1 Million+ on Target Audience Analysis Training

On October 12, media reported the Canadian army was behind the fake wolves letter. Coincidentally, the same day came further news of target audience analysis training for the Canadian military by a company led by a key executive formerly of Strategic Communication Laboratories, or SCL. This was the parent firm of Cambridge Analytica (both firms now defunct), made infamous from its work on the 2016 U.S. election and the 2016 Brexit referendum.[125]

Emma Briant, a respected U.K. academic researching propaganda and the influence industry, writing in *Organized Crime and Corruption Reporting Project*, explained how the MilStratCom group within DND Public Affairs spent more than $1 million over two years for Emic Consulting to train about 40 people, mostly PAOs, in six-week courses in audience analysis and behaviour-change techniques. The request for proposal noted DND would retain "proprietary usage" of the methodology and courseware to develop a program "that will support Joint Targeting, Information Operations and Strategic Communications in the long-term."[126] The training was

[123] See Emma Smith, "No, A Pack of Wolves Has Not Been Unleashed in Rural Nova Scotia," CBC, October 8, 2020, https://www.cbc.ca/news/canada/nova-scotia/gray-wolves-reintroduction-misinformation-fake-letter-lands-and-forestry-warning-1.5755595; and Haley Ryan, "Nova Scotia Army Reserves Behind Fake Letter of Released Wolf Pack," CBC, October 12, 2020, https://www.cbc.ca/news/canada/nova-scotia/nova-scotia-army-reserves-behind-fake-letter-of-loose-wolf-pack-1.5759266. Accessed January 2, 2022.
[124] See https://www.rt.com/op-ed/505716-canada-psyops-wolves-facebook/. Accessed January 2, 2022.
[125] Emma Briant, "Opinion: Governments Have Failed to Learn from the Cambridge Analytica Scandal," Organized Crime and Corruption Reporting Project, October 12, 2020, https://www.occrp.org/en/37-ccblog/ccblog/13225-governments-have-failed-to-learn-from-the-cambridge-analytica-scandal. The following day, Canadian media picked up this story. See David Pugliese, "Canadian Military Spent More than $1 Million on Controversial Propaganda Training Linked to Cambridge Analytica Parent Firm," Saltwire, October 13, 2020, https://www.saltwire.com/nova-scotia/news/canadian-military-spent-more-than-1-million-on-controversial-propaganda-training-linked-to-cambridge-analytica-parent-firm-508717/. Accessed January 2, 2022.
[126] See https://buyandsell.gc.ca/procurement-data/tender-notice/PW-20-00920078. Accessed January 2, 2022.

part of the overall Defence strategic communications initiative being established "to influence the attitudes, beliefs, and behaviours of audiences."[127]

The DND responded that the training was needed to "develop customized and effective communications campaigns," claiming that National Defence, with more than 950 people in or supporting Public Affairs, "does not have the ability to deliver in-house training on audience research and strategic communications campaign planning."[128] The activity – the second iteration of the training taking place in the midst of a pandemic that put a premium on the time of communications practitioners – struck some insiders as a questionable and expensive undertaking in the face of other competing priorities. A former senior military Public Affairs officer even argued in the media that such training threatened the institution's credibility.[129] Following the media coverage, Public Affairs leadership decided not to exercise the provision for an additional, two-year, non-competed $1 million+ contract to the firm.

The Military Public Affairs Employment and Enhancement Concept (MPAEEC)

The proverbial straw that broke the camel's back came in early November 2020, with another exclusive story by Pugliese, about the National Defence initiative to establish a strategic communications group featuring Public Affairs working alongside IO and PSYOP practitioners to influence behaviours, including overseas and domestic audiences.[130]

The front-page headline – "Canadian military to establish new organization to use propaganda, other techniques to influence Canadians" – coming so soon after previous revelations about military strategic communications misfires, again raised concerns inside and outside DND. "No such plan has been approved nor will it be," Sajjan's press secretary stated in the article. The Opposition's defence critic was also quick to express condemnation (Fig. 6-1) and social media commentary was decidedly negative.[131] So too was the reaction inside DND: the overt and tacit support that had sustained the initiative in the face of negative publicity crumbled, as very senior leaders now took the time to read and digest the long-gestated plan.

As explained in Chapter II, the MilStratCom vision sought through organizational change to create greater separation between military practitioners focused on the CAF and war-fighting, and

[127] National Defence, Military Public Affairs Employment and Enhancement Concept (October 2020 draft), 7.
[128] Order Paper Question 570, tabled in House of Commons, Canadian Parliament, May 2021.
[129] See David Scanlon, "Fight the Information War Without Sacrificing Canadian Values," *Ottawa Citizen*, October 27, 2020, https://ottawacitizen.com/news/national/defence-watch/fight-the-information-war-without-sacrificing-canadian-values. Accessed January 2, 2022.
[130] David Pugliese, "Canadian Military to Establish New Organization to Use Propaganda, Other Techniques to Influence Canadians," *Ottawa Citizen*, November 2, 2020, https://ottawacitizen.com/news/national/defence-watch/canadian-military-to-establish-new-organization-to-use-propaganda-other-techniques-to-influence-canadians. Claims within Defence that this article was wrong were silenced when senior leaders viewed the organization chart for the group that included IO and PSYOPS officers and practitioners within the Public Affairs organization, reporting to military PAOs and ultimately to the civilian official responsible for DND/CAF Public Affairs. The civilian official quickly cancelled the positions.
[131] The tweet by Opposition defence critic James Bezan: "Conservatives are extremely concerned about reported proposal for 'Defence StratCom' and whether this is the best use of our defence dollars. Will Harjit Sajjan publicly commit to not 'weaponizing' CAF public affairs?!" See Figure 6-1. November 2, 2020. Accessed November 2, 2020.

civilian practitioners focused on "recruiting and other benign institutional priorities."[132] That sat poorly with senior leaders, as did the notion that the military Public Affairs plan "to shape how we train, equip, structure and fight in the information domain" was based on the problematic IO concept paper prepared at CJOC and proposed to be a key initiative line of effort.[133] As it turned out, senior leaders at Defence thought the key Public Affairs line of effort should be conducting better public affairs.

The stakeholder, media and internal reaction suggested CAF leaders had not ensured effective oversight, direction and guidance of a complex institution-wide effort. The reaction also confirmed the battlefield had not been sufficiently prepared with media and internal or external audiences to make the case for why reform was needed, what was to be done or how guardrails would be in place to ensure separation of PA/IO/PSYOPS on domestic operations and activities and thereby protect institutional reputation (Fig. 6-2).

The need for military communications reform had certainly been the subject of presentations and discussions at a variety of conferences and schools over the years.[134] These tended to be validations of pre-determined intent, rather than a deliberate engagement strategy seeking to learn from thought leaders their best advice on what to reform and how, to ensure the effort would also find favour in civil society. Even in a strictly hierarchical organization like Defence, a substantial number of experienced serving practitioners remained ill at ease at what they were seeing and hearing about the initiative. Other practitioners from the IO and PSYOPS community were concerned but found no real mechanism to weigh in: "My supervising officer was horrified watching this," recalled one officer. "There were Influence Activity folks who felt that this was a full-speed ahead train about to derail. There were merits in the idea, but it was the wrong approach."[135]

The MilStratCom group's calculated risk to avoid attribution in the media about the initiative had come home to roost. Trying to mount a counter-attack from scratch, especially given that the story elements were correct, was an insurmountable challenge. Even the MilStratCom initiative lead seemed to acknowledge as much, lamenting "we were exploring uncharted territory … Innovation is sometimes prone to being misunderstood."[136] It turns out the initiative led by Public Affairs and in no small measure about Public Affairs was not underpinned by a communications strategy. As Briant observed, "Militaries need to stop blaming the public for not understanding such efforts. This decision to blame others reveals that it is the military itself which doesn't understand the

[132] MPAEEC, 16.
[133] MPAEEC, 4 and 18.
[134] See https://www.youtube.com/watch?v=KLs_zPDs8wo. Accessed March 15, 2022.
[135] Exchange with officer in the Influence Activity community, February 2022.
[136] David Pugliese, "Canadians Shouldn't Be Viewed as 'Targets': Military Initiative to Aim Propaganda at Public is Shut Down," *Ottawa Citizen*, November 13, 2020, https://ottawacitizen.com/news/national/defence-watch/canadians-shouldnt-be-viewed as-targets-military-initiative-to-aim-propaganda-at-public-is-shut-down. Accessed January 2, 2022.

communication landscape well enough to recognize why audience boundaries and clear communications matter."[137]

By this point, there was overwhelming evidence of ambiguous policy; problems with authorities, governance and oversight; confusing lexicon; and insufficient understanding and agreement about whether, if and how to employ military capabilities in domestic operations meant for use against foreign adversaries. The aggregation of negative media articles throughout the initiative, but during 2020 in particular, had notably damaged confidence in the DND/CAF's public communications effort at home and abroad. This threatened both the CAF's operational success and institutional ability to progress the Defence program. The inability to provide sufficient public explanation about the individual events reported in the media or to adequately explain the overall initiative demonstrated the MilStratCom effort was adrift and floundering. The CDS had seen enough. Vance ordered an end to the project and directed that overall guidance for a re-alignment of the effort be expedited.

[137] David Pugliese, "Government Efforts to Counter Propaganda Risk Undermining Public Trust," *Ottawa Citizen*, December 11, 2020, https://ottawacitizen.com/news/national/defence-watch/government-efforts-to-counter-propaganda-risk-undermining-public-trust. Accessed January 2, 2022.

V: Reviews are in, and Institutional Leaders Begin to Respond

The pandemic brought daily challenges enough for National Defence leaders, including fighting the impacts of disinformation and misinformation, without the CAF itself being the subject of media coverage and online discussions about the veracity of its communications. The stories (see Appendix 2) piling up, suggesting untoward activity, threatened confidence in the institution. Military leaders were also unhappy at the systemic inability to generate positive momentum on how to evolve the MilStratCom initiative and frustrated at reading in the media information about the project that did not square with what staff was telling them. The institutional (NDHQ), operational (CJOC HQ) and military strategic communications/military Public Affairs effort (based in ADM PA) had veered way off-piste from Vance's original intent five years before. The effort needed recalibration, and urgently.

"Canadians must have absolute confidence in knowing that we completely understand our role in informing the public space of our initiatives and activities," wrote Laurie-Anne Kempton, the new assistant deputy minister for Public Affairs, in an early November 2020 all-staff note announcing the decision to end the MilStratCom initiative.[138] "They must know that they are not targets … The draft [Military Public Affairs] Employment Concept paper is not in line with my vision for ADM(PA) and is not supported … our efforts to enhance the formal range of duties of Public Affairs Officers into the Information Operations/Influence Activities domain have come to an end." Finally, a senior official had explicitly captured Vance's verbal intent to enhance and protect public confidence in Defence communications. This included assuring a clear demarcation between Public Affairs and the variety of influence activities available to the military drawing on threat, coercion and deception meant for contested expeditionary operations. The media duly reported the shutdown.[139]

Resetting the MilStratCom Initiative

A week later, Vance and Thomas jointly issued written, formal, internal guidance to reset the full suite of information-related capability initiatives, detailing 74 tasks to 13 offices.[140] Notably, this was the first time during the entire project that senior leaders had issued such written direction. The key strategic outcome desired was to, "Change the institutional mindset so that the value of communicating actions is an integral element of our deliberation, planning and decision-making from the start."

The carefully chosen initiative title shed light on three key features that suggested hope for a new way ahead from the path taken to that point. First was the clear expression that the top military and civilian leaders intended an outright reset of the overall effort and not just a tweak of the

[138] E-mail by Laurie-Anne Kempton to Public Affairs staff, November 5, 2020.
[139] Pugliese, November13, 2020.
[140] "CDS/DM Planning Guidance - Enhancing Operational and Institutional Communications: Resetting the Information-Related Capability Initiatives," November 12, 2020.

various initiatives under way. Second was the need for a holistic examination and treatment plan to improve all the relevant capabilities across the Defence portfolio: this was not just a Public Affairs problem set nor should it be their lead, and responsibilities and accountabilities were therefore assigned throughout the organization. Third, the guidance overtly expressed that both the CDS and the DM had equities in the informational space, setting out the need for an integrated, enterprise-wide joint military/civilian effort connected to wider government communications policy.

The guidance acknowledged "recent missteps in the application of IO policy and conduct of related activities during domestic operations and training exercises" created confusion about intent, eroded public confidence and risked jeopardizing Defence's ability to tackle legitimate threats in the information environment.[141] The document identified four constraints that were impeding reform efforts: insufficient guidance for authorities and responsibilities that led staff to work independently, resulting in an overall lack of oversight and accountability; a lack of policy and doctrine; problematic lexicon; and a "learn by doing" mentality. Typical of the communications strategy to that point, the document was not publicly released at the time or leveraged internally or externally to inform the still-ongoing debate. As a result, an otherwise notable initiative that might have started to reframe the MilStratCom initiative narrative flew under everyone's radar.

The reset guidance tasks were informed by a good sense by the staff of what the three reviews examining the information-related missteps were likely to find. These three – plus a new, fourth review in December, were nearing completion within a few weeks of each other.

The Army Review of Influence Activities Function + the "Fake Wolves" Summary Investigation

The army's IO function and PSYOPS capability – despite the *Strong, Secure, Engaged* defence policy commitment – had never been a priority for, nor a particular interest of, a succession of army senior leadership. The "fake wolves" exercise in September 2020 suggested that a broader examination of the army-only influence activity (IA) function (including CIMIC, IO, PSYOPS) was in order: that started in late October and was completed by the end of January 2021. No one was under any illusion the review findings would be anything other than grim. The reality was worse.

The review detailed a long litany of shortcomings in the influence activity capability: no doctrine since 2004; no dedicated scenarios at the unit level where training took place; no field publications, unlike other branches in the army; no other army capability with a similar employment concept; no NATO countries with a similar structure to Canada; split responsibilities for where training expertise could be found, unique in the army; no course to educate the leadership "on how to properly employ their elements … in both a domestic and operational

[141] Ibid., 7.

context"; training that did not take place during times favourable to reservists, on which the whole force generation model depended; no career path for practitioners; no analysis of training needs; no standard equipment lists and little functional equipment; and a lack of qualified personnel in the regular force to offer guidance or mentorship … for a start.[142]

These macro army-level findings closely mirrored the situation at the Halifax Rifles Influence Activity Squadron, the unit that was the subject of the "fake wolves" summary investigation. The investigation determined the member responsible for the letter had no training in IA or PSYOPS – but neither did more than two-thirds of the group. Standard procedures or protocols for the production of PSYOPS products did not exist. The situation was a comedy of errors, a consequence of the army's longstanding systemic neglect, including how to recruit, train and employ the practitioners, non-existent oversight by the IO functional authority in the CAF and no army or institutional champion. As the commander of the division wrote following his endorsement of the investigation: "No longer can these designated IA sub-units be left on their own to train themselves. They simply do not have the capabilities, training and expertise to do that at this point."[143]

The Compliance Assessment Report – Intelligence Support to OP LASER

In July 2020, DND/CAF's intelligence command was directed to look into the military's information-gathering activities (defined as intelligence, so excluding routine activities like media analysis reports), during support to civil authorities during the COVID pandemic. Personnel collected information via social media, including about key regional actors to "determine what they were communicating in the information environment" to inform briefings and support operational planning and decision-making by commanders. The review found that CJOC HQ (specifically, the section that prepared and issued the IO annex) and two subordinate groups, including the Joint Task Force HQ in Toronto, unknowingly did not comply with all requirements associated with intelligence activities.[144]

The influence activity practitioners had been pressed into new work on no notice, mostly working from home, with a different reporting relationship (unusually, to G2 Intelligence rather than G3 Operations). They lacked access to the relevant policies and were unfamiliar with how those applied to their work. The review found that for activities such as reporting on the Black Lives Matter movement, it was difficult to link some of the information-gathering activities to the requirements of the mission.

[142] Canadian Army Doctrine and Training Centre, Review of Influence Activities Function Within the Canadian Army, January 27, 2021. (See ATIP A0525769).
[143] 5th Canadian Division Headquarters, "Endorsement – Summary Investigation Report, Unauthorized Release of Training Scenario Material into Local Community," November 2020. (See ATIP A0487469).
[144] A summary of the Canadian Forces Intelligence Command, "Compliance Assessment Report Intelligence Support to Op LASER Report" is included in the CDS/DM Directive – Response to Reviews of Information Operations and Influence Activities (June 9, 2021) that was shared with select media and reported on.

It can be fairly said that most likely there was no malicious intent, but the episode pointed again to the lack of appropriate policy and practitioner/leader training about how to use information-related capabilities meant for overseas conflict in a benign domestic setting. Group members raising concerns about their work to the media should also have been a sign to commanders that the junior and mid-level practitioners were concerned about the direction things were headed.

The Command Process Review (the Gosselin Report)

The fact that CJOC HQ had been oblivious to the potential reputational damage to the institution of issuing an IO annex for a domestic operation, and assumed authorities to act without first seeking senior staff input continued to weigh on the CDS. Consequently, and fresh from the reset guidance discussions, in early December 2020 Vance directed a review to learn how events had transpired and what lessons could be derived. Retired Maj.-Gen. Daniel Gosselin had three weeks to do research and submit findings, which he did on December 28.[145]

The reviewing officer came to the subject without any background knowledge of the various information-related capability initiatives, narrow terms of reference and limited time over the Christmas period during a pandemic to prepare the study. In spite of these challenges, the detailed report gave a clear picture of the timeline of events and circumstances within an extremely busy headquarters managing the CAF's response to the pandemic, as well as all other operations. The report found the IO annex was issued on April 8, five days after the main operations order; the CDS was alerted to the subject by his staff on April 19 and expressed immediate concern, the next day directing any such activity be stopped; the annex was first "administratively rescinded" by CJOC then formally cancelled 10 days later; and (unnamed) senior officers within the chain of command at NDHQ didn't know until June that the document had even been issued.

While the command process review concluded there was no evidence anyone conducted unsanctioned activities, Gosselin did set out three worrisome findings. He assessed that CJOC had "loosely interpreted" the extant Joint Info Ops Policy from 2018 and "liberally interpreted" the Crown prerogative for domestic operations, assuming authorities they did not have.[146] He also determined that draft policies under development but particularly the Joint IO Force Employment Concept was "… critical – and even dismissive at times – of the contribution of the strategic level….such a key concept document, personally endorsed by [Rouleau], may become much more authoritative then initially envisaged." Alarmingly, Gosselin found a "palpable, dismissive attitude … where strategic-level [NDHQ] advice and considerations were considered to be of limited relevance for those responsible to plan and conduct operations [at CJOC]." This was a disturbing assessment of command climate by an experienced and respected general officer

[145] Gosselin, Command Process Review – CJOC Information Operations Directives, December 28, 2020.
[146] This author takes a different view: it is not that staff took liberties with the scope of the extant policy, but as a designated support command they were in fact implementing the CDS/DM direction to conduct information acts during "all defence activities and operations … to induce, reinforce, convince, encourage or even coerce them [approved target sets] in support of [government of Canada] objectives." While wrong to do so, CJOC was doing what (a poorly formulated) policy directed. From Joint Info Ops Policy (2018), 3. Subsequent CDS/DM direction in June 2021 made clear the need to formally clarify the issue in a revised Joint Info Ops Policy.

and spoke volumes about the operational mindset and distinctive "operators know best" culture that had driven and enabled the MilStratCom initiative all along.

However astute the observations, due to time pressure the report was challenged to offer many detailed corrective measures except to recommend reviews and changes to related policies, and to update doctrine and directives to eliminate inconsistencies and make responsibilities clearer. The report also called for the creation of separate instructions to clarify CAF information-related authorities and activities during domestic operations.

The command process review had been commissioned by the CDS and so the report's disposition – the "what to do now?" – was the CDS's purview. On December 23, Prime Minister Justin Trudeau announced that Adm. Art McDonald would take over from Vance, and so the MilStratCom problem set was McDonald's burden, along with everything else.[147] The handover period between the outgoing and incoming officers was several weeks shorter than anticipated, a transition made more challenging than usual by the pandemic and the restrictions this imposed.

Those with equities at stake from the various unreleased reviews and proponents of an activist IO approach now had to deal with a new CDS who, by virtue of his naval service and background, was less familiar than his army counterparts with the various information-related concepts, lexicon, policies, activities and prospective applications. This is because all the influence-related capabilities were owned and force-generated by the army (except Public Affairs, which was well represented throughout the CAF). The Gosselin report findings and the army's role in influence activities did not sit well with the new CDS, who questioned much. Chastened army leaders, including Eyre, the commander, were told to prepare for more high-level discussions about the subject, and the army feared the entire capability was now potentially at risk.[148]

Those briefs did not take place because on February 2, 2021, Global News broke the story of sexual misconduct allegations against Vance, beginning a dizzying series of media revelations against nearly a dozen CAF general and flag officers. On February 24, McDonald voluntarily stepped aside when informed the military police were investigating him. The situation was described by the newly appointed acting CDS Eyre as an "existential issue" and culture change initiatives became the leadership focus for months. At the same time, overseas operations continued and the pandemic response was still job one, as was responding to floods and fires. It was an elevated institutional and operational tempo in difficult work circumstances, including several high-profile CAF leadership changes. The subject of information-related capabilities was hardly top of mind.

By late spring 2021, the situation was as follows: the MilStratCom/military public affairs initiative ended in November 2020, with instructions that PA would do PA, not IO or IA. Planning guidance to reset the initiatives had been issued but was not publicly acknowledged or communicated. Some related, incriminating documents had been released thru Access to Information, but had not yet been reported on, and more ATI requests on a broader range of material, including the

[147] See Murray Brewster and David Cochrane, "Vice-Admiral Art McDonald Named New Chief of the Defence Staff," CBC, December 23, 2020, https://www.cbc.ca/news/politics/art-mcdonald-chief-defence-staff-1.5853182. Accessed January 2, 2022.
[148] Confidential discussion with attendee, February 2020.

four reviews (intelligence gathering, "fake wolves", the army's influence activity capability and the command process review) were incoming. All reviews and investigations had been finished for months but the findings and institutional response had not been internally socialized broadly nor publicly communicated. Routine PSYOPS and IO training across the army was on hold pending clarification of senior leader intent. Further delay in publicly communicating some response to the long-finished reviews risked additional negative media publicity with the prospect of losing the narrative for good. Indecision also added to the staff's confusion and work churn about what senior leaders wanted to do to take stalled work forward.

CDS/DM Response to Information-Related Capability Reviews

Consequently, on June 9, 2021, Eyre and Thomas quietly issued the CDS/DM Directive – Response to Reviews of Information Operations and Influence Activities. Prompted by a series of media queries about the status of the four outstanding reviews and conscious of upcoming releases of information thru ATI, the directive was sent to select journalists two weeks later, the same day that Parliament recessed for the summer. National media were quick to report about the contents.[149]

The directive was a frank admission of "missteps" that "caused reputational damage to the DND/CAF" and offered forthright, albeit condensed explanations of the four reviews, (as summarized earlier). Two findings from the directive offer particular insight into what senior leaders had by then concluded about the MilStratCom initiative. First was the assessment that, "…sometimes insular mindsets at various echelons have eroded public confidence in the institution and create confusion about the necessity to enhance our ability to conduct operations in the information environment." This was pointed criticism of units in the army and of army personnel at joint headquarters, but mainly of CJOC HQ and its leadership at the time under Rouleau.[150]

And, in a stark admonishment of the by-then-disbanded MilStratCom/military Public Affairs group within ADM PA, the CDS and DM determined: "The effort to expand the formal range of duties of Public Affairs Officers into the IO/IA domain, including the draft MIL PA Enhancement

[149] See Murray Brewster and Ashley Burke, "Military Campaign to Influence Public Opinion Continued After Defence Chief Shut it Down," CBC, June 24, 2021, https://www.cbc.ca/news/politics/psychological-warfare-influence-campaign-canadian-armed-forces-1.6079084, Accessed January 2, 2022, in which a Defence spokesperson said information about the reviews would be released "in the coming week or so" (as of April 2022, that was still not the case). With rumblings of a federal election being called and Sajjan under regular pressure over his handling of the military sexual misconduct file, there was no appetite for proactively releasing more information about the review findings or having to answer questions of accountability while the House of Commons was in session. David Pugliese also covered the story from a different perspective. See Pugliese, "Military Violated Rules by Collecting Iinformation on Canadians, Conducting Propaganda During Pandemic: Report," *Ottawa Citizen*, June 24, 2021, https://ottawacitizen.com/news/national/defence-watch/military-violated-rules-by-collecting-information-on-canadians-conducting-propaganda-during-pandemic-report. Accessed January 2, 2022. In September 2021, Pugliese was the first to report details of the Gosselin Command Process Review, obtained through Access to Information, nine months after the report was finished. See Pugliese, "Military Leaders Saw Pandemic as Unique Opportunity to Test Propaganda Techniques on Canadians Forces Report Says," *Ottawa Citizen*, September 27, 2021, https://ottawacitizen.com/news/national/defence-watch/military-leaders-saw-pandemic-as-unique-opportunity-to-test-propaganda-techniques-on-canadians-forces-report-says. Accessed January 2, 2022.

[150] There was still turmoil in the senior ranks at this time. Coincidentally, five days after the review response was issued, Rouleau, then the vice-chief of the defence staff, stepped down following criticism of a golf excursion with Vance, and the head of the navy.

and Employment Concept paper, *were incompatible with [Government of Canada] Communications Policy, and the DND/CAF vision, mission and principles of Public Affairs*." [italics added]. These words were a real gut-punch for those involved in the five-and-a-half-year-long initiative, but a relief to military and civilian practitioners inside the organization concerned about where things had been headed. It may have been some consolation that senior leaders at least acknowledged that not providing strategic direction much earlier had hobbled the effort from the start.

The directive re-affirmed the intent and tasks of the November 2020 guidance and prioritized three key tasks. First was to publish an updated version of the 2018 Joint IO Policy to more clearly spell out applications of that policy on domestic operations. Second was to finalize a Defence Strategic Communications directive – a new and welcome lexicon change suggesting a DND/CAF/government effort, not just a MilStratCom undertaking by the military. Third was to issue revised DND/CAF social media policy including new direction on social media engagement. These policies were optimistically forecast to be finalized by the end of 2021, but as of February 2022, were not.

It took some time to effect a course correction, but the institutional response was an articulation finally, of some senior leader written guidance, some good words, some good intent and some good actual and proposed action. At least, on paper. The challenge to realizing such bold goals was that the inherent features that allowed independent, unconnected, untoward initiatives to evolve and metastasize remained the same. This included suboptimal governance mechanisms, weak functional authorities, an allergy to external expert advice and a tepid engagement strategy, but mostly, traditional thinking still about how to organize the inform-influence-persuade assets. To better compete in the information environment, Defence needs a re-imagination – not tweaks – of communications policy, doctrine, structure, governance, oversight, leader engagement, process, force generation and force development. Rising to that challenge, the next section sets out 10 lessons observed from the MilStratCom initiative and 20 suggestions for the way ahead.

Table 2: A Comparison of Approaches – A Top 10 List

How The MilStratCom Initiative Transpired vs.
A More Effective, Alternative Model

1	*Verbal senior CAF commander's intent provides sufficient authority and direction and is much faster than trying to articulate in writing.* Written senior DND/CAF direction and guidance confirms explicit aims, objectives and responsibilities for all concerned. This shared understanding speeds project implementation.
2	*Title the initiative MilStratCom (later, MilPA), led by PAOs, established within ADM(PA), but without authority, accountability or responsibility for any information-related capabilities.* Create a defence communications task force reporting to the vice-chief of the defence staff, led by a senior official or officer of at least two-star rank. Provide full-time staff with relevant backgrounds to expedite changes in legal, policy and planning frameworks and training.
3	*Bottom up, practitioner-led. All information-related capabilities work in discrete and separate silos. Each functional area moves as quickly or as slowly as interest, capacity and capability allow.* Treat initiative as a complex project; staff a project management office accordingly. All related policy, doctrine, training, education and resource needs are subject to DND/CAF-wide approach.
4	*Existing governance and oversight are sufficient; more of each impedes speed of progress.* Effective governance requiring regular initiative-wide reporting (at least quarterly) is an important forcing function that disciplines an enterprise-wide initiative and holds it accountable. This keeps senior leaders informed, engaged and invested in the process and outcomes.
5	*A CAF-only initiative, with DND PA transformation as a separate line of effort (civilians are "corporate PR agents"); few touch points with whole-of-government (WoG) partners.* Any serious effort must be DND/CAF-wide, military-civilian integrated and ideally nested within a WoG initiative that Defence should fund as a contribution to national security.

6	*Approach the communications reform effort from a war-fighting perspective.* Focus the effort on the full spectrum of DND/CAF roles and activities from domestic operations to overseas operations up to and including combat, as well as DND institutional requirements.
7	*Keep the same lexicon, organizational structure, force-generation approach, force-employment process, governance and oversight means for all info-related capabilities – just add money.* Don't just assign more people and give more money to do more of the same thing. Re-imagine Defence communications; rethink structure, reset initiatives, reorient staff and organizations, refocus efforts and restore lost credibility and reputation. Evolve the lexicon.
8	*Begin separate information-related capability occupational analyses (examine the jobs and tasks in each field, which determines the training needed) at the back end of the reform effort.* An occupational analysis is the natural activity to begin such a capability reform initiative; cut the time to do these by half by forming integrated teams of full-time subject matter experts.
9	*Brief friendly stakeholders to seek validation for pre-ordained strategy and actions.* This approach results in confirmation bias. There is now an impressive knowledge base in related fields resident in academia, think tanks and civil society from which to draw advice from outside experts to help develop policies and discover opportunities for co-operative partnerships.
10	*Initiative leads intuitively know what their own capability gaps are and what is needed to improve. Baseline and benchmark assessments only slow progress that is needed now.* Detailed baseline and benchmark reviews are key to confirming and validating strengths, weaknesses, opportunities, resources, outputs, capability gaps and training needs. Information from such an enterprise-wide perspective informs organizational structure and priority of work. Absent a holistic assessment, all lines of effort are working in stovepipes.

VI: The Military Strategic Communications Initiative: 10 Lessons Observed

1. Ensuring excellent institutional communications that satisfy domestic audience needs first is a core capability requirement: this should have been the MilStratCom focus, but was not.

Doing well on the home front is a necessary first condition for an effective Defence communications capability and provides a foundation to do well in deployed contested operating environments. The Defence Public Affairs group was under considerable stress and strain after years of operating at a continuous high tempo, with relentless demands for external and internal communication services including for creative, innovative content. The pandemic, plus a brutal domestic and international operations tempo, exacerbated all these challenges. Oblivious to this situation, the MilStratCom initiative pulled people, money, time and effort from the PA functional authority's ability to support real-time DND activities, CAF operations and to progress its own transformation effort. This negatively impacted the capacity to plan, manage and conduct quality public affairs for the Defence enterprise at the strategic and operational levels. Not appreciating this was happening and arresting that trend during the five-and-a-half-year initiative was a DND/CAF leader and ADM(PA) miscalculation of the first degree.

2. Institutional/corporate (DND) comms in large measure relate to military (CAF) operational comms and vice versa: these are not mutually exclusive undertakings, but two sides of the same coin.

By its very name, MilStratCom expressed a limited vision for change and reform, with a focus on military practitioners and (ostensibly, but not really) on the strategic, rather than on evolving communication policy and capabilities Defence-wide. The effort to brand and distinguish practitioners as either military "information warriors" or civilian "corporate PR agents" was divisive. The naming conventions diminished the contribution of civilian leaders and practitioners, and in practice meant a uniformed PAO fell either in the "we do overt influence alongside IO" camp (with inducements of better training, higher assessment ratings and possible assignment out of the hard slog of day-to-day PA); or was a naïve body who didn't get it, with the associated career implications. This created high tension among long-serving career Public Affairs officers, leading some to debilitating moral injury, and also caused real angst among many in the non-PA practitioner community. Defence communications work best when the military and civilian effort is joint and integrated, leveraging each other's skills and experiences, even if these tend to be quite different, for the full range and suite of missions.

3. Absent written senior-level direction and guidance, effective governance mechanisms, real oversight and expert external advice, initiative leads will hear what they want to hear.

The lack of written direction and guidance from the CDS and DM to launch and shape the initiative proved highly problematic. Without a common understanding of the aim, desired outcomes, tasks, constraints, limitations, accountabilities and responsibilities for an institution-wide effort of such complexity, initiative leads were free to interpret and translate senior leader verbal intent in a way most favourable to their personal or parochial interests. There was no requirement to regularly report about overall progress to an oversight body and thus no meeting minutes/decision notes to inform involved actors of the state of overall work. This stifled active discussion and muted constructive criticism since "the CDS said this is what he wants" was hard to disprove or counter by those not in the room whenever any relevant verbal exchanges took place. This worked as a tactic but was poor strategy since it meant a very small number of people could claim knowledge of the overall initiative or its key lines of effort. Draft concept papers disguised as approved policy added further confusion: the November 2020 CDS/DM Guidance and the June 2021 Acting CDS/DM Directive noting this, were solid efforts to correct these shortcomings, but came after the fact.

4. Too many leaders left practitioners to try to work it all out on their own for too long.

Responsibility for the slow failure of the MilStratCom initiative over more than five years ultimately rests with the collective senior military-civilian leadership at Defence, and the force development function under the vice-chief of the defence staff, which establishes conditions to evolve related capabilities within the CAF force structure. The widely accepted need is for the institution to set information effect more clearly at the core of DND/CAF planning and thereby enable more strategic, deliberate and proactive execution of all activities. Instead, it was easier for senior military leaders to consider strategic communications mostly as an issue of practitioner training for the affected functions to sort out rather than as the wicked problem it was, since the latter would require fundamental changes in leader mindset, education and training, institutional process and organizational capabilities. For there to be any chance of success, the initiative needed to be approached as an enterprise-wide task force-level effort with dedicated project management planning and policy support.

5. Terminology in use was and remains seriously detrimental to the effort.

Many of the terms that litter the lexicon – "targeting," "shaping," "adversary," "threat," "battleground," "non-kinetic munitions," "influence activities," "psychological operations," "influence," "changing attitudes and behaviours," even *strategic* communications and

information operations – are burdened with perceptions, fears and associations of tools, assets and weapons used wrongly in the past. Even operationally seasoned senior military leaders and practitioners still grapple with information-related capability lexicon, concepts and applications: here, the lack of updated doctrine is a major contributing factor. These terms do not translate well to CAF activities at home nor with partner agencies and departments, let alone media or the public. It is not up to outsiders to learn, understand and grow comfortable with the concepts and terms – it is for Defence to better explain and evolve terminology where needed to more accurately say what is meant.

6. There was a lot of 'blame and complain,' but little 'explain.'

In the face of uncomfortable media articles, criticism or unsatisfactory outcomes about Defence initiatives or programs, the first instinct most often within military leadership is not self-reflection about the communication effort but to cast blame – on leakers, the Opposition, the Ombudsman, the Parliamentary Budget Officer, the DM, the minister, commentators, but mainly the media for a lack of understanding of whatever is at issue. Enhanced education in certain quarters in Defence of civics and appropriate military-civilian relations is required, including how the DM and minister do have real equities in the operational space – just like the CDS has equities in the institutional space. So too is a greater appreciation of the role and place of a critical media and stakeholders in a democracy, and how to manage that relationship better.

7. First things didn't happen first.

Being associated with a new initiative that has senior leader attention is attractive to staff, especially if there are few funding constraints or a requirement to regularly report to governance bodies to confirm that priorities and effort are aligned with direction. Less interesting is the time-consuming foundational work like first defining overall training needs, refreshing policy, establishing a governance and planning framework and changing outdated regulations: the MilStratCom team dismissed these as DND institutional remits. To accelerate progress, many corners were cut and too many actors enabled to learn by doing. Proceeding with a sense of urgency and concurrent activity is a welcome tactic but this effort did not progressively evolve along well-practised project management principles including first knowing how much capability existed, what each produced, what this cost and what were the real collective gaps to be fixed. Ensuring oversight is especially important in fields like StratCom, IO and PSYOPS with its modest depth and breadth of experience among practitioners, planners and commanders.

8. The same people doing the same thing the same way with the same processes, same policies, same doctrine, same governance and same oversight mechanisms will take you to the same place as before.

The November 2020 Guidance and the June 2021 Directive are just task checklists if major changes are not made to how DND/CAF policy/doctrine and joint forces are developed in the informational space, or how related initiatives are co-ordinated across the institution. An effort of such complexity and impact enterprise-wide needs stronger functional authorities; more effective governance; a non-PAO lead agent to help guard credibility; and to draw on expert, independent, unbiased external advice as a forcing function against the current mindset.

9. It does not naturally follow that what works for one entity in a particular operating environment will work for another entity in different circumstances.

For several reasons, what works well enough at a NATO military planning HQ or in another country like the U.S. or U.K. does not necessarily work equally well in Canada at a strategic political-military integrated National Defence Headquarters. Policy, structures, authorities, accountabilities and responsibilities all need to be highly attuned to national needs, requirements, laws, policy, experience and the Canadian information environment.

10. Be able to practise what you preach before proselytizing.

The information-related capability communities did not successfully plan and execute persuasive campaigns to convince Defence insiders of their respective initiative road maps. Judging by the tone of media coverage, journalists and external stakeholders did not understand the initiative intent, either. Public Affairs practitioners in the MilStratCom group did not do the basic elements of the craft they otherwise do on any other big task – prepare a communications strategy with a narrative and key messages, develop multiple knowledgeable spokespersons, empower subject matter experts, conduct media engagement and create compelling content to inform audiences. Neither did influence practitioners conduct target audience analysis of their own to determine key internal stakeholders or to identify constituent beliefs, culture and attitudes that would challenge the ability to build understanding, engagement and support for their effort. This was a stunning lack of awareness by practitioner communities of the operating and information environment, and how niche military language would resonate inside Defence and outside their cloistered communities. After more than five years of trying, the initiative could still not be neatly explained inside the CAF to garner wide senior leader support and to generate actual progress. That does not bode well for the idea that these capabilities are ready to lead inform-influence-persuade-coerce activities institution-wide.

VII: Re-Imagining Defence Communications – 20 Recommendations

Strategic communications is a wicked enterprise-wide problem that needs to be managed like a complex project, requiring senior-most leader engagement and effective governance.

Information is one of the four elements of national power and underpins the other three (diplomatic, military, economic). More militaries are also recognizing information as a domain and in Canada, as the central theatre of operations and activities. In today's operating environment, effective Defence communications is not only a vital asset, but arguably is an existential institutional requirement.

Nearly seven years after the initiative began, there is still no DND/CAF StratCom policy or doctrine and even an initiating directive to frame the problem set has proven elusive. There is no strategic joint command and no viable functional authority to effectively oversee the DND/CAF effort. Governance is weak, key policies are more than 20 years old and senior leaders have refused to invest senior, experienced operator talent into the initiative.[151] Simply put, the conditions for success in the DND/CAF in this field have not been established. Assigning a leader of sufficient rank and experience at the head of a task-tailored group to evolve the institutional mindset and turn clusters of capabilities into a joint, integrated capability is imperative. Communicating strategically needs to be a mindset that is baked into the institution, not sprinkled on, or suddenly important only when an issue is about to go public.

Recommendations:

1. Structure the effort as a complex project. Establish a full-time Defence communications task force charged with hyper-accelerating action to change relevant legislation, revise policy, build training and undertake force development. This group should include the leading subject matter practitioners from inside DND/CAF with representation from legal, training development, force development, finance, policy, doctrine, the three services and Special Forces, and with support from expert external advisors.

2. Assign high quality general, colonel and staff officer operator/planners to this functional area, demonstrating action to back up the words that the informational space is central to all Defence operations and activities.

3. Develop and implement effective governance, oversight and accountability mechanisms to help manage and support information-related capability reform.

[151] Wark, drawing on the experience of recent reforms in Canadian intelligence, suggests "accountability, especially as conducted by independent, external review bodies established through legislation, must be central to the conduct of information operations in the domestic sphere." From "The Pen and the Sword: Information Operations and the Domestic Environment," 16.

Understand the baseline.

In an organization as large and diverse as Defence, it is not uncommon that some group somewhere is producing something another group needs or could use (such as information environment analysis), but who and where that is may not be known. Over the course of the MilStratCom initiative, it did not occur to first identify, detail and confirm the resources already engaged in information-related capability activities, what they were doing, the work processes or the collective capability and output gaps. This lack of shared understanding had pernicious consequences, including organizations all independently seeking additional resources for discrete capabilities for themselves, risking duplication of effort and fuelling a zero-sum competition for new positions. Notably, with more than 950 people working in or for Defence Public Affairs and 10 squadrons in the army's influence activity field (mostly part-time army reserve), the problem set in no small measure is a resource allocation challenge, not insufficient investment.

Recommendation:

4. Understand and document the collective resource, task, training and capability gap baseline across the breadth of the information-related capabilities. Knowing this is critical to determine work priorities, resource levels, investment needs and identifying impediments in organizational structure and work processes.

Determine the benchmark nations and organizations in these fields and why that's the case.

Leaders of note in their respective fields include the U.S. Marines (operations in the information environment); NATO HQ Brussels (large political/military institution communication strategy and execution); the U.K. military (strategic communications mindset); and the U.K. government Communications Service (practitioner development, building resilience against mis/disinformation). The 2022 Russia-Ukraine war also provides a dramatic case study to derive information-related capability lessons from which to understand the poor performance of the former and the notable performance of the latter.

Recommendation:

5. Identify the entities that obtain good outcomes in the inform-influence-persuade-coerce space and figure out why that is. What are the success factors and are they unique to that entity, or can they be applied here? If not, why not? What conditions were needed to enable those successes? Knowing what works well elsewhere and why helps inform what is more likely to work in the DND/CAF.

Re-imagine, don't just tweak, Defence communications.

It has proven very difficult in the DND/CAF – and NATO nations writ large – to organize effort and match big ambitions with actions in the information environment because by policy and doctrine that space is unbounded. Some disaggregation is required. It is time to admit certain immutable truths – IO as a descriptor and organizing concept does not work well; influence activities (IA), a construct unique to the Canadian army that combines IO, PSYOPS and CIMIC, is ineffective as currently configured as is the associated IA task force; PSYOPS is broken; and the model that attracts, trains and employs these people based on the army reserve is conceptually the least effective force-generation option. This situation is confirmed by the four information-related capability reviews of 2020 and the resulting CDS/DM direction and guidance documents, the operational concept papers prepared by CJOC and considerable practical experience. Fiddling on the margins of a fundamentally unsound foundation may offer some satisfaction to leaders of being seen to do something, but does not change the underlying fundamentals nor improve the situation.

Recommendations:

6. Give up "information operations" as a term and staff function: information operations are operations. Instead, create more manageable groupings of like capabilities by separating the highly technical means (space, cyber and electronic warfare, under a specialist not generalist IO staff) from those that actually perform the inform-influence-persuade cognitive ways activities. At the same time, replace the stand-alone IO officer staff function model with a new operational communications sub-specialty that embeds more robust knowledge in plans staff and commanders throughout the entire joint force.

7. Give up PSYOPS as currently conceived, structured and practised in Canada – this is a First World War, Second World War and Korean War anachronism. In Canadian and NATO doctrine, PSYOPS is a white capability – the content produced is truthful and attributable. In other words, this is public information for local audiences on expeditionary operations, contested or otherwise. This capability needs to be re-rolled, renamed and made joint (air force and navy, not just army). Doing this has massive potential for better PA, IO and CIMIC for the joint force and almost certainly will result in personnel savings after redistribution.

8. Give up "influence activities" as a concept, term and task force name. Currently, the CAF (and NATO) organizes information-related capability based on inform- or influence-related intent: instead, organize assets around attribution. If content is publicly attributed, that's Public Affairs and put those assets there. If content is not attributed, that falls in the deception and special capabilities lane, which belongs in the current and future operations shops: staff accordingly. CIMIC is a valuable asset on overseas missions but especially at home as domestic operations needs increase. This needs to be a stand-alone, joint sub-specialty outside the influence-activities orbit and augmented: CIMIC is perfectly suited to be force-generated by the reserve force.

Change the force generation model.

The information environment is a tremendously challenging space in which to manoeuvre and is a 24/7 commitment. Assigning responsibility to the army reserve force to recruit personnel for IO, IA and PSYOPS, then providing spotty training with no career path is a recipe for continued suboptimal results. This is a well-trod road and no amount of time or money with this approach can possibly elicit notably better outcomes. Public Affairs is a purple trade because practitioners come from all services and both the regular and reserve force: any colour uniform in the occupation can support any of the other services. The occupation is also mainly regular force supported by equally trained reservists, a model for others to emulate.

Recommendations:

9. Develop a joint force concept for information-related capabilities.
10. Create an operational communications sub-specialty for officer practitioners and for non-commissioned officers available to both the regular and reserve forces and build specialized training for commanders.
11. Change responsibility for generating practitioners skilled in operational communications to the regular force from the reserves. Each of the navy, air force and army reserve should have a trained cadre of operational communications practitioners with job and promotion opportunities to remain in that sub-specialty over the course of a career.

Base the renewed Defence communication effort on a foundation of excellent public affairs.

Here is a harsh reality for IO practitioners, information warriors and all operator influence enthusiasts: nearly all strategic communications problems or examples at DND/CAF are in fact a result of suboptimal policy, questionable leadership decisions, poor execution or lack of communications effort – usually, two or more. Rarely, or perhaps never, are bad outcomes the result of a lack of authorities to conduct IO/IA/PSYOPS. Public trust in the DND/CAF is the critical enabler for every activity and every operation, domestic and otherwise: leadership-driven PA is the key capability that most directly impacts institutional credibility and organizational reputation. It is also the key function linking communications between the CAF and civilian oversight, including the DM and minister's office; whole-of-government partners such as the Privy Council Office, Treasury Board, Global Affairs, the Prime Minister's Office and other departments and agencies; and the media plus stakeholder communities.

The PA branch has been unable to evolve practitioner skills fast enough to match institutional needs and commander expectations. In large measure, this is due to constraints on how the occupation is managed, since PA is grouped with personnel selection officers, training

development officers and musicians under the Canadian Defence Academy as the training authority. This needs to change.

The relevant DND policies also need to urgently evolve with the times – the related Queen's Regulations and Orders (QR&Os) are from the year 2000 but read like they were developed in the 1960s. Six of the nine extant PA Defence Administrative Orders and Directives (DAODs) are the originals from 1998. Defence needs to realize the internet is not a passing fad and urgently evolve relevant policies and legislation to meet current needs and requirements. Leadership should also realize the Public Affairs function needs an injection of skilled, non-PA, CAF planners and managers, and external support to help make sustainable reform happen faster.

Recommendations:

12. Strengthen the PA functional authority by accelerating an update of the relevant QR&Os and DAOD 2008 Public Affairs series and give ADM(PA) managing authority to decide how best to allocate Public Affairs assets throughout the DND/CAF. Specifics should be informed by findings of a long overdue review of the PA function with its nearly 1,000 personnel.

13. Establish ADM PA as the training authority for the Public Affairs and unclassified imagery functions (like intelligence, military police, medical and special forces).

14. Upgrade practitioner skills and knowledge by borrowing an idea from the U.S. and German militaries, who provide extended loan to industry opportunities for deserving members and who then bring that experience back. Education at staff college or a related master's program is fine, but assignments with industry, think tanks (like Atlantic Council or Carnegie's Partnership for Countering Influence Operations) and select civil society groups leading reform in this space will grow skills faster and expose military practitioners to leading thinkers, techniques and technologies in use in the private sector.

Use 'proactively inform' or even 'principled persuasion,' not 'ethical influence' as a guiding tenet for domestic public affairs.

"Ethical influence," proposed as a guide for domestic public communications at Defence would irrevocably harm DND/CAF's reputation and public trust in the institution. In addition, labelling all Canadians as targets so their behaviours can be influenced in deliberate campaigns with the wide array of assets at Defence's disposal is abhorrent policy. No reasonable person disputes the need or merit for information communicating intent to be more engaging and effective to better connect with specific key audiences to explain Defence needs and requirements, defend the institution against mis-or disinformation, encourage recruiting or to convince troops to get vaccinated, to stop smoking or to get into better shape. Honest communications should be Defence's watchword.

Communicate, communicate, communicate about the reform initiative.

If passive is the default DND/CAF communications approach for this work, then be prepared for the same unfortunate outcomes. The five-and-a-half-year MilStratCom experience demonstrates that reactive communications is a losing strategy. The November 2020 CDS/DM Guidance and the June 2021 Acting CDS/DM Directive, if leveraged, offer a good start to addressing the media and public narrative gap. Defence will need a serious campaign effort to recover internal and external confidence and trust in the reform effort.

Seek genuine external stakeholder engagement and expert advice and encourage active listening.

A brave new world of very impressive civil society groups, organizations, academics, skilled researchers and think tanks is now focused on the information problem set. Defence should deliberately engage knowledgeable groups in a structured, persistent, inform-educate-and-learn campaign. The point of engagement is not to seek the like-minded to validate immutable views and opinions borne of just a military perspective, but to challenge conventional approaches and undercover potential biases and groupthink. Instead, capability leads need to elicit constructively critical insight in structured sessions with experts in their respective fields to help develop related policy and capability, thereby building external confidence in the reform effort.

Recommendations:

15. Create a formal external advisory group featuring thought leaders and critical thinkers in the related fields.
16. Create a media forum to rebuild trust with and relearn military-media relations.
17. Create an advisory group of retired practitioners to contribute to branch reform efforts.

A deliberate strategy to directly involve more than the DND/CAF in the reform effort.

Proactively mitigating the effects of mis-and disinformation is a national security imperative. This demands a holistic approach to upgrade whole-of-government capability and help build resilience against information-related threats to the country. Given its relative wealth and breadth of significant capabilities, resources and experience compared to other departments, such an initiative should be financed by, but not led by Defence.

The capacity in Canada and NATO more broadly to communicate strategically with greater effect will continue to muddle along so long as a StratCom mindset and process-based capability is not purposefully built into the NATO defence planning process (NDPP). The NDPP sets out military

capability the Alliance needs from nations and through negotiation, what nations agree to provide. There are currently 14 NDPP planning domains covering many discrete capabilities and none relates to inform-influence-persuade functions. This is a longstanding shortcoming of vision by NATO military authorities deserving of North Atlantic Council attention – if StratCom is not a stated obligation and requirement, many nations will be reluctant to invest.[152]

Recommendations:

18. As a contribution to national security, Defence should fund the creation of a unit in the Privy Council Office dedicated to building resilience in civil society against mis- and disinformation, and to dramatically improve government communications capability and capacity.

19. Defence should provide a major investment in the mobilizing insights in defence and security (MINDS) initiatives to foster, develop and enable new, sustainable capability and capacity in universities and civil society, in fields related to information environment studies and research.

20. Defence should provide military and civilian staff or contracted support as voluntary national contributions to NATO to accelerate the definition of StratCom capability to be included in the NATO Defence Planning Process.

[152] See https://www.nato.int/cps/en/natohq/topics_49202.htm. Accessed February 15, 2022.

VIII: Conclusion

A virus of mis-, dis- and malinformation invades and infects our lives daily. The volume of vitriol is increasing as malign influence operations by state, non-state and even by domestic actors have become widespread and commonplace. This deliberate effort to undermine peace, order and good government – as well as life, liberty and the pursuit of happiness – makes the work of elected leaders in democratic societies particularly challenging and places formidable new demands and stressors on institutions. There is no vaccine for this virus. But one prescription can help build resilience and fight back – a fit-for-purpose, leadership-driven communications capability highly attuned to the innate value of institutional credibility and organizational reputation.

Recent events have demonstrated the centrality of government communications to the body politic, and how vital it is to be able to effectively manoeuvre in the information space. Re-imagining the communications function in the federal government and at National Defence is now a national security issue of the first order. In particular, DND/CAF need to finally put paid to their belief that the information domain is the central theatre of operations and activities and get demonstrably better, smarter and faster at communicating strategically. This does not mean doing more with less, or even doing more with more – both have been tried, with limited success. The solution set is also considerably more involved than the advice to "just let the troops tell it like it is; they will never let you down."

Additional investments in the current construct will realize smaller or even negative marginal incremental returns and come with huge opportunity costs: measurable effects and outcomes less than the cost of investment is not just an unsustainable business model, but in a defence context, is a recipe for decisive defeat against adversaries who get it. In other words, doing more of the same thing gets National Defence to a worse place faster.

Re-imagining Defence communications will require developing a construct that meets the particular demands and challenges of the information environment of today and tomorrow. Tinkering with structure, policy, governance and lexicon designed in the pre-internet age does not move the yardsticks forward. It's time to accept that the internet is not a passing fad. Doing notably better means communication effect is embedded as an organizational mindset with distinctive and efficient processes, including leader engagement, effective governance and oversight, substantial capabilities and robust capacity. Communicating strategically needs to be baked in from the start, not sprinkled on. Re-imagining the function means resetting the various initiatives, reorienting staff and organizations, refocusing efforts and restoring lost credibility and reputation. This has significant structure, authorities, policy, regulatory, training and education implications – but if Defence likes the outputs and outcomes from its information-related capability investments now, then keep doing the same thing.

Ideally, we would wish to conclude that the five-and-a-half-year-long MilStratCom initiative was a series of unfortunate, unconnected events and activities by well-intentioned people doing their level best, the effort veering off track slightly and attracting some undeserved media attention, and with just a tweak needed to set right. However, this is not the case. Events show distinct,

worrying patterns of behaviour and intent and a disturbing culture and mindset among certain quarters of the CAF. This was DND/CAF leadership's wilful negligence, military practitioner hubris and communications malpractice.

There is good news, though, including that some positive action has taken place. Defence has put forward clear and reasonable explanations in internal reports of how missteps occurred. The MilStratCom initiative as constituted at the time was stopped and clarifying direction issued. This suggests leaders now may be more attuned to the need for improved oversight, direction, guidance and active management of the functions. This is a policy, authorities, governance, planning framework and resource distribution challenge, not a lack of resources problem. And Public Affairs, the core capability needed to help get out of the current quicksand, is fundamentally a solid and proven performer during war, conflict and peace – though massively underappreciated and undervalued, and in real need of a get-well program. All in all, the situation offers an opportunity for a real reset.

The bad news is that to make progress DND/CAF-wide, operator culture and mindset in certain quarters need to change. Leaders need to understand that the same-same approach and structure gets the same-same outcomes. A way needs to be found to work through a contemptuous attitude to oversight, direction and guidance by superior HQs; overcome disdain for civilian authority, civilian advice and civilian practitioners; eliminate the allergy to external advice; and restore the military-media relationship. A public recommitment to changing this aspect of CAF culture would be helpful. As David Mulroney, former deputy minister and ambassador to China observed: "Underlying the profoundly disturbing revelations of abuse of power and trust, and of widespread sexual harassment, is a culture of high-level dishonesty. This conclusion is inescapable. Healthy communications flow from a healthy organization, one that is committed to telling the truth. And that starts at the top."[153]

The ugly news is the demanding operational tempo and overload of big issues happening concurrently will continue. The continuing pandemic and its after-effects, the culture change priority, the Russian invasion of Ukraine with the multiplicity of second- and third-order consequences and other major initiatives including a defence review, mean for the foreseeable future the conduct of routine business will be a considerable challenge, stress and strain. The capacity and capability to take on new initiatives and reform efforts of an institutional nature is at a historic low. The means to do so must be found.

To briefly recap events, then. The June 2017 *Strong, Secure, Engaged* defence policy that set out right and proper intent to develop targeting prowess and offensive IO capabilities missed a notable opportunity to explain the compelling need for broader communications reform and innovative thinking in the information domain. Spring 2018 was a watershed period. The April 2018 CDS/DM Joint Info Ops Policy established that IO was "applicable to all defence activities and operations," and directed commanders to undertake activities to "induce, reinforce, convince, encourage or even coerce" targeted individuals and groups. This policy remains extant, though

[153] Exchange by David Mulroney with the author, April 15, 2022.

CDS/DM direction was issued in June 2021 to amend it and more clearly define the policy's relation to domestic operations.

The tweet storm in spring 2018 by a senior Public Affairs officer against commentators mildly critical of Defence, including labelling one journalist a Russian propagandist and calling the media discussion and parliamentary debate about the Mali mission "nonsensical" was a turning point. To insiders, this appeared an overt expression of the new Joint Info Ops Policy and practical applications of the ethical influence concept proposed as a new tenet for Public Affairs. By adopting the MilStratCom title as their own, PAOs in ADM(PA) and CJOC suggested they had responsibility and oversight for all the information-related capabilities. Unwittingly or not, this directly connected Public Affairs with information operations, influence activity, PSYOPS and military deception including on domestic operations – if these were not the remit of a chief, director and director general MilStratCom, who else possibly could be responsible? These and other developments split practitioners into three camps: civilian staff, military staff thought to be against the effort and thus corporate PR agents, and those for the effort and thus prospective information warriors. This approach degraded DND/CAF's ability to more effectively manage strategic and day-to-day public affairs.

In early November 2020, Vance directed that the MilStratCom/MilPA initiative be shuttered, mainly because of a series of media articles over several years detailing embarrassing missteps by Defence including but not limited to Public Affairs, that could no longer be ignored or explained away by the various initiative leads. Vance's decision was also acknowledgment of angst in DND/CAF about the direction of work, the lack of obvious progress or evidence of better outcomes that could be attributed to the initiative. In mid-November, Vance and Thomas jointly issued guidance to reset all the information-related capability initiatives. In June 2021, Eyre and Thomas issued a directive summarizing the findings of four internal reviews looking into related matters and assigned additional tasks and priorities. Notably, these instructions did not change how this work was to be done or managed, but merely added new work to a construct that had proven unable systemically to conduct such a project.

It was routine for initiative leads to dismiss the periodic media coverage about missteps as biased and to marginalize practitioners who expressed concerns internally. It bears highlighting then, the key findings from the four internal reviews and the two related CDS/DM documents to illustrate institutional leadership conclusions:

- "It is clear that the development of the various information related capabilities have suffered from a lack of institution-wide strategic level direction and guidance to grow a joint CAF and integrated DND/CAF capability that is professionalized, sustainable and governed by appropriate authorities and oversight."

- "CJOC loosely interpreted the 2018 [Joint] *IO Policy*, particularly its understanding of what was included with the Crown Prerogative … to conduct information operations in Canada."

- "It is clear that the authoritative direction [Joint IO Policy] was liberally interpreted … and that risks identified by Policy, [Judge Advocate General] and PA staffs were dismissed, which was also indicative of a mindset by some leaders at the HQ."

- "Concept documents have been championed by senior CAF leaders as surrogates for obsolete doctrine …[and] mistaken as authoritative."

- "It is difficult to link some of the information gathering activities of the [precision information targeting team] to the requirements of the [OP LASER pandemic] mission."

- "No longer can these designated [influence activity] sub-units be left on their own to train themselves. They simply do not have the capabilities, training and expertise to do that at this point."

- "A palpable dismissive attitude was detected … where strategic level advice and considerations were considered to be of 'limited relevance' for those responsible to plan and conduct operations."

And, most remarkably, in June 2021:

- "The effort to expand the formal range of duties of Public Affairs Officers into the IO/IA domain, including the draft [concept paper] was incompatible with Government of Canada Communications Policy, and the DND/CAF vision, mission and principles of Public Affairs."

That Kempton, Eyre and Thomas judged the MilStratCom/MilPA initiative and the associated vision concept document to be "incompatible" with government policy was a stunning indictment of the effort. Any misstep, be it an indecorous tweet against media by a PAO in the heat of the moment, a story about "fake wolves" or the issue of an IO annex for a domestic operation, would not on its own necessarily have suggested anything systemically untoward about, nor directly connected to, the MilStratCom initiative. Stepping back and considering holistically the aggregate of activities and documentation, though, makes clear how the CDS and DM would conclude the initiative was at odds with government policy and Defence PA principles and values.[154] Actions

[154] It is fair to ask who bears responsibility for how events unfolded over the course of the MilStratCom experiment – and to wonder where was senior leadership when all this was going on? The admission in June 2021 by the senior military officer (Eyre) and senior civilian official (Thomas) that the effort "suffered from a lack of institution-wide strategic level direction and guidance" is key. As the initiative catalyst, a key actor in the 2017 *Strong, Secure, Engaged (SSE)* defence policy, co-signer of the 2018 Joint IO Policy, and CDS throughout the MilStratCom initiative, Vance bears his share of responsibility for what transpired. The extent to which these are faults of omission or of commission is debatable. To his credit, Vance was the first CDS to decisively commit to trying to improve the way Defence strategically communicates, including making investments to do so. When informed of the ground truth of problems, he acted – sending the safeguarding information instruction back for further work, directing the IO annex be rescinded and commissioning a report to learn lessons from that, ending the MilStratCom initiative and issuing detailed guidance to reset the various lines of effort.

Not unreasonably, Vance expected subordinates, especially general officers from the CJOC/operator and Public Affairs communities, to brief him and senior leadership truthfully, faithfully and objectively, especially as the initiative stalled and obvious problems mounted. In too many cases over too long a time, this trust was misplaced. With no one person explicitly designated to grip the multiple work strands, responsibility and

like the senior military Public Affairs officer advocating ethical influence as an operating tenet for PA; establishing IO and PSYOPS positions in and reporting to Public Affairs; considering institutional communications as "faceless, distant, and incapable of effective interaction and listening" and recruiting as a "benign institutional activity"; spending more than $1 million for Public Affairs officers to learn behavioural change techniques in the face of other pressing reform priorities; using social media to attack journalists and commentators critical of Defence and parliamentarians engaged in debate about the CAF; seeking to improve CAF military communications at the expense of DND institutional communications; promoting the draft Joint IO concept calling for the targeting of all Canadians and anticipatory authorities to conduct IO; and supporting the establishment of Defence StratCom "to influence the attitudes, beliefs and behaviours of audiences" – eventually did not sit well with senior military and civilian leaders.

Defence Communications Reform

Re-imagining Defence communications requires an explicit new vision for the future, an enterprise-wide leadership effort, decisive action, seriously improved governance and additional executive competence in the information-related capabilities. It will require a conceptual framework to deliberately set information objectives and effect more clearly at the core of strategic planning, operational design and the execution of activities, so that everything the institution says, signals or does, can be, to the extent reasonably possible, aligned to support national interests and approved objectives.

The DND/CAF should wish to enhance its capabilities and with sufficient capacity to be demonstrably more effective in the information environment in all spheres of activity, both domestic and in expeditionary operations, up to and including combat. This vision should entail an enterprise-wide, joint, integrated military/civilian capability that is professional and governed by updated policies and legislation, appropriate authorities, quality governance mechanisms and

---

accountability were diffuse – there was "no one neck to choke." The lack of a project management/task force approach, effective governance or oversight, or of independent external advisors was a serious detriment. This situation should have been of particular interest to the various vice-chiefs of the defence staff given that office's responsibility for force development, but the group remained quietly in the margins throughout, perhaps because of the frequent turnover of vice-chiefs.

The staff most directly involved in the initiative had much to gain from realizing their respective visions and were blind, or wilfully insensitive, to the potential and real institutional and reputational impact. They understated risks and overstated risk mitigation strategies and so forged ahead, enabled and encouraged by a select few senior operators, mostly but not exclusively at CJOC. For most of the time the MilStratCom initiative was underway, the top Public Affairs civilian official (assistant deputy minister level) was a former senior military PAO, who was supportive of the effort.

Jody Thomas assumed responsibilities as DM DND after *Strong, Secure, Engaged* and shortly before co-signing with Vance the Joint Info Ops Policy in April 2018. The timing suggests not wanting to rock the boat so early in her tenure by pushing back on a big CAF want tied to the Defence policy. Besides, the MilStratCom initiative was decidedly a CAF effort driven by military officers, who were not partial to any intervention by civilian officials in the scheme. Harjit Sajjan, the Defence minister for nearly all the time of the MilStratCom initiative, appears to have asked few questions even in the face of regularly embarrassing media coverage about the subject and was oblivious, incurious, misled or a combination of the three.

real oversight and informed by expert outside independent advisory group(s) of knowledgeable stakeholders.

The DND/CAF will increase its chances of success post-MilStratCom initiative by considering the various recommendations presented earlier, including these three in particular:

1. This is a complex project and should be treated, organized and staffed as such. Create a Defence communications task force with full-time DND/CAF representation of subject matter experts from legal, training development, policy, doctrine, strategic joint staff and force development shops, alongside skilled practitioners from the relevant disciplines and drawing on an outside expert advisory board. Staff all information-related initiating directives, framework documents and proposed policies through this clearing-house to avoid task fratricide and provide policy consistency and coherence. This will accelerate progress and reduce the risk of individual lines of effort working at cross-purposes. The task force lead should be an experienced official, outside practitioner or general officer of at least two-star rank.

2. Conduct a review of the PA functional authority with its nearly 1,000 personnel to find where longstanding staffing conventions could change to improve outcomes: such a study has not been done in at least 30 years, if ever, and is long overdue. Further, the federated model of communications needs to change to a management authority structure similar to that for the legal and military police branches. Currently, the communications head is accountable to the CDS and DM for the function but does not have authority to make decisions about the allocation of people, priority of work and training needs across the DND/CAF.

3. Create an operational communications sub-classification and qualification course for officers and non-commissioned members in both the regular and reserve forces. Make this a joint course and a joint capability.

    - End Information Operations as a name, process, lexicon and organizing concept. Split the technical capabilities of IO (cyber, space, electronic warfare) from those that work in the cognitive domain (inform-influence-persuade) to make this a more manageable space.

    - Reprofile the army's influence activity capability and the Influence Activity Task Force into operational communications. Take CIMIC out of the influence activity stream, make it joint and increase its complement.

    - Disband PSYOPS as currently configured: re-allocate positions to CIMIC, operations staff (being trained in operational communications) and to Public Affairs.

Effective communications underpin every successful DND/CAF initiative and activity. We should hope that the lessons from recent international and domestic events, as well as the MilStratCom initiative experience, will generate new impetus and renewed effort for a reformed construct of the communications function. At the DND/CAF, institutional leaders should insist that public trust, organizational reputation and institutional credibility be a guiding feature of that effort, its operations and activities, domestic or international, in combat or otherwise. In the contemporary information environment, a suboptimal communications function is a strategic liability at the best of times and possibly an existential threat to the institution.

Appendix 1: The Military Strategic Communications Initiative in Canada – A Timeline and Explanation *('Top 10' Notable in Bold)*

Sept. 22, 2015: *Ottawa Citizen* reports on CAF initiative to "weaponize" PA.
The first public expression of intent by new CDS Gen. Jonathan Vance to improve MilStratCom.

June 7, 2017: *Strong, Secure, Engaged* defence policy released.
Initiatives include developing offensive IO; enhance army reserve role in IO and PSYOPS.

July 19, 2017: North Atlantic Council endorses *MC0628 NATO Military Policy on Strategic Communications*
Places info-related capabilities under one communications director at NATO military HQs. This organization structure, wrongly, is used as a model for the CAF MilStratCom initiative.

Sept. 8, 2017: Brief to Armed Forces Council about PA Operationalization and Military StratCom.
Leaders agree general concept to modernize IO, targeting, influence activity in army reserve, and more effective PA on operations. By default, PA becomes the MilStratCom initiative lead.

January 2018: Senior PAOs adopt MilStratCom titles and promote these inside and outside of CAF.
By definition, these titles tell DND/CAF that PA is the initiative and proponent lead for StratCom, IO, PSYOPS, military deception and other information-related capabilities.

April 3, 2018: *CDS/DM Policy on Joint Information Operations* issued
Establishes that IO is a "command responsibility," is "applicable to all defence activities and operations" and is included in the "earliest stages of planning and throughout" operations.

April 2018: Senior military PAO sends multiple tweets critical of media and of parliamentary debate.
This suggests overtly confrontational approach to media and stakeholders critical of Defence is a deliberate strategy that was overtly or tacitly supported by senior leadership.

June 13, 2018: Publication of "What if the Pen is a Sword?" paper (Canadian Forces College) by Col. Jay Janzen.
Introduces ethical influence concept for PA; desire to leverage skills of IO for domestic ops.

Feb. 10, 2019: Distribution of "How We Fight," hand-written by Lt.-Gen. Michael Rouleau, Commander CJOC
Influential think-piece setting out intent to better prepare CAF for contested operations, with the informational space as a central theme. This guides work at CJOC and leads to development of draft concept papers (reviews in 2020 and 2021 conclude these "untested and experimental concept documents" were "surrogates for obsolete doctrine").

April 2019: *CDS Directive for the Implementation of Joint InfoOps/MilStratCom Capability* draft circulates.
Suggests developing capability and using it will occur at same time (learn by doing). This document does not gain traction and is abandoned in favour of the MPAEEC (see June 2020).

April 26, 2019: CAF *MilStratCom/PA Operationalization Force Development Plan* draft circulates.
Notes MilStratCom "may challenge boundaries of current national policies"; sets out authorities to conduct IO, PSYOPS, MilDec on Canadians and allies (removed in next draft). This effort does not gain traction and is abandoned in favour of the MPAEEC (see June 2020).

January 2020: *Pan-Domain Force Employment Concept (PFEC)* draft circulates more widely (CJOC lead).
Translates "How We Fight" into framework by CJOC to shape how military forces are developed and how capabilities/needs are defined. PFEC is "a driver of change starting today." New defence policy in all but name; document informs intent, work and priorities for the CAF's main operational HQ.

January 2020: Joint Information Operations Force Employment Concept (JIOFEC) draft circulates.
Initially meant as an annex to the PFEC and very nearly issued by CJOC in June 2020, but is not. The JIOFEC shows the real gulf between operator/practitioner mindset and acceptable, viable practice. Suggests document will "allow us to shift from a responsive posture to an anticipatory posture vis-vis policy, authorities, mandates and capabilities." Explains how in any engagement "there exists only targets," with use of kinetic or non-munitions planned by the "information age warrior." This document continued to be modified by staff throughout 2020 and into 2021, featuring still in the 2021-2022 DND/CAF Departmental Plan. Following multiple internal reviews and

investigations of MilStratCom missteps, as of April 2022, CJOC now considers the document "obsolete."

April 8, 2020: CJOC issues IO annex for OP LASER, the CAF's COVID-19 pandemic response.

May 2020: CDS Guidance on Strategic Military Planning draft circulates among senior military staff.
Effort to translate the PFEC into formal CDS guidance (that is, direction); sets out various defence lines of effort and 15 strategic initiatives with strong emphasis on "prevailing in combat against adversaries" over domestic defence considerations. This guidance does not get approved.

Spring 2020: MilStratCom organization chart includes IO and PSYOPS positions reporting to PAOs in ADM(PA). With budget re-allocations, the MilStratCom initiative also becomes the best-funded group within the PA functional authority (excluding unit that spends on recruit advertising).

June 2020: *DAOD 2006-1 Safeguarding Information* draft sent back to drawing board by Vance.
Effort to create new classification to limit release of unclassified information from DND.

June 2020: Military Public Affairs Enhancement and Employment Concept (MPAEEC) begins wide circulation.
Acknowledges the JIOFEC is framework for all CAF activities and operations; cites it five times.
Seeks to create new military unit and organizationally separate military from civilian PA practitioners.
Notes Defence StatCom will "influence the attitudes, beliefs and behaviours of audiences."

July 20, 2020: *Ottawa Citizen* first reports on IO annex: "Information Operations Pandemic Campaign Quashed After Details Revealed to Top General"
Defence minister directs a review of intelligence collection activities.

Summer 2019: MilStratCom/MilPA Ethical Framework drafts circulate for comment.
Effort to codify conduct for military PA practitioners (but not civilian PA staff or commanders). Raises suspicions as to why the DND/CAF Code of Values and Ethics is not sufficient.

Oct. 12, 2020: Media reveal army reserve PSYOPS unit in Nova Scotia is behind "fake wolves" letter.
Leads to summary investigation of the incident and a broader review of influence activity capability (IO, PSYOPS, CIMIC) by the army.

Oct. 12, 2020: *Organized Crime and Corruption Reporting Project* reveals CAF paid $1 million+ for target audience analysis training mostly for PAOs, to a firm led by a former long-time senior executive of Strategic Communication Laboratories, the parent company of Cambridge Analytica.

Nov. 2, 2020: *Ottawa Citizen* reports on the Military Public Affairs Enhancement and Employment Concept draft paper ("Military Want to Establish New Organization to Use Propaganda to Influence Canadians").

Nov. 5, 2020: Vance directs end to MilStratCom/MilPA initiative begun in 2015
Kempton to staff: "Our efforts to enhance the formal range of duties of Public Affairs Officers in the Information Operations/Influence Activity domain have come to an end"; "the draft [MPAEEC] is not in line with my vision for ADM(PA) and is not supported."

Nov. 12, 2020: CDS/DM Enhancing Operational and Institutional Comms Planning Guidance is released.
First time for written senior military-civilian direction on the MilStratCom effort; seeks to reset all related initiatives; assigns 74 tasks to 13 organizations.

Nov. 13, 2020: Media report the MilStratCom initiative is shut down

Nov. 27, 2020: Former top military PAO publishes *Defence Watch* article: "Fight the Information War Without Sacrificing Canadian Values," critical of "pattern of ethical breaches" at ADM(PA).

Mid-December 2020: Strategic Joint Staff-led StratCom Options Analysis Working Group starts meeting.
First time since initiative begins that wide representation from all directly affected DND/CAF stakeholders gather to collectively develop options. Dissolves in early days of pandemic.

Dec. 28, 2020: Command Process Review examining how IO annex was released submitted to Vance.
Key Findings: CJOC HQ "loosely interpreted the 2018 IO Policy"; "liberally interpreted" authorities to conduct IO on domestic operations"; "palpable dismissive attitude … strategic-level advice and considerations considered to be of limited relevance for those responsible to plan and conduct operations."

Jan. 27, 2021: Army's Influence Activity Capability Review is finalized.
Key Findings: lack of IO/PSYOPS policy, training, equipment, career path and oversight.

June 9, 2021: *CDS/DM Directive – Response to Reviews of IO and IA* is released internally.

Key Findings: "Sometimes insular mindsets at various echelons have eroded public confidence in the institution"; "conduct of IO on a domestic operation without explicit CDS/DM direction or authority"; "effort to expand formal range of duties of Public Affairs Officers into the IO/IA domain, including the draft MIL PA Enhancement and Employment Concept paper, was incompatible with [government] Communications Policy … and PA principles."

June 24, 2021: Media report on CDS/DM Directive (June 9, 2021) and outcomes of the various reviews.

Document is sent to select media same day House of Commons breaks for summer session, meaning the minister of Defence is spared questions about it in Parliament.

Aug. 12, 2021: *Ottawa Citizen* reports on army investigation of "fake wolves" PSYOPS exercise, obtained via ATI.

Sept. 27, 2021: *Ottawa Citizen* reports on December 2020 Gosselin/Command Process Review, obtained via ATI.

Appendix 2: Selection of Media Headlines about the MilStratCom Initiative 2020-21[155]

David Pugliese, "Canadian Military to Crack Down on Leaks of Unclassified Information After Embarrassments to Government," *Ottawa Citizen*, June 8, 2020.

Scott Taylor, "Canadians Not Interested in Military Spy Games," *The Hill Times*, June 28, 2021.

David Pugliese, "Canadian Forces 'Information Operations' Pandemic Campaign Quashed After Details Revealed to Top General," *Ottawa Citizen,* July 20, 2020.

David Pugliese, "Team with Canadian Military Intelligence Unit Data-mined Social Media Accounts of Ontarians During Pandemic, *Ottawa Citizen*, July 21, 2020.

Haley Ryan, "Nova Scotia Army Reserves Behind Fake Letter of Released Wolf Pack," CBC, Oct. 12, 2020.

David Pugliese, "Canadian Military Spent More Than $1 Million on Controversial Propaganda Training Linked to Cambridge Analytica Parent Firm," *Ottawa Citizen*, Oct. 13, 2020.

John Ismay, "Canadian Military's Wolf Exercise Alarms Nova Scotians," *New York Times,* Oct. 16, 2020.

Scott Taylor, "Canadian Military's Public Affairs Branch Has Weaponized Itself Into Self-destruction," *Saltwire*, Oct. 27, 2020.

David Pugliese, "Canadian Military Wants to Establish New Organization to Use Propaganda, Other Techniques to Influence Canadians," *Ottawa Citizen,* Nov. 2, 2020.

Kit Klarenberg, "Wolves, Social Media & Tactics from Afghanistan: Canadians Should Be Worried about Their Government's Bizarre Psyops Exercises," *Russia Today*, Nov. 5, 2020.

David Pugliese, "Canadians Shouldn't Be Viewed as 'Targets' – Military Initiative to Aim Propaganda at Public is Shut Down," *Ottawa Citizen,* Nov. 13, 2020.

Scott Taylor, "DND Propaganda Project Shut Down," *Esprit de Corps*, Nov. 16, 2020.

Scott Taylor, "When the Military Dares to Deceive, No One Wins," *The Hill Times*, Nov. 18, 2020

[155] This non-exhaustive sampling of media headlines across a spectrum of Canadian and international media during 2020-21 shows how the initiative was being characterized five years after it began. This compendium is one compelling measure of performance and consequence of the initiative's insufficient communications approach and engagement strategy. The accrued effect on organizational reputation and institutional credibility is not reasonably calculable – but the tone of media headlines and actions by DND/CAF senior leaders suggests the impact was notable. The deliberate strategy to avoid media and not explain the reasons for reform and how the CAF was trying to adapt to be more operationally effective in the information environment permitted negative narratives to take root and gave oxygen to conspiracy theorists and malign actors about Defence's intent. That the situation was allowed to devolve to this point illustrates the lack of direction, guidance, governance and oversight by the DND/CAF senior leadership from the earliest days of the initiative.

David Pugliese, "Canadian Military Intelligence Monitored Black Lives Matter Movement, Claiming Pandemic Justified Such Actions," *Ottawa Citizen*, May 11, 2021.

Murray Brewster and Ashley Burke, "Military Campaign to Influence Public Opinion Continued After Defence Chief Shut it Down," CBC, June 24, 2021.

David Pugliese, "Military Violated Rules by Collecting Information on Canadians, Conducting Propaganda During Pandemic: Report," *Ottawa Citizen*, June 24, 2021.

Press Progress, "Military Admits It Made 'Errors' Aiming Propaganda at Canadians and Spying on Black Lives Matter Groups," June 25, 2021.

Scott Taylor, "Military's Foray on Using Propaganda on Canadians Out of Line," *Saltwire*, June 28, 2021.

David Pugliese, "Military Propaganda Exercise that Caused Panic about Wolves on the Loose 'Lacked Oversight' Investigation Finds, *Ottawa Citizen*, Aug. 12, 2021.

Jeremy Appel, "Canada's Military is Spying on Canadian Citizens," *Jacobin,* Aug. 17, 2021.

Mack Lamoureux, "Conspiracy Theorists are Salivating Over a Canadian Military Psy-Op Report," *Vice*, Sept. 23, 2021.

David Pugliese, "Military Leaders Saw Pandemic as Unique Opportunity to Test Propaganda Techniques on Canadians, Forces Report Says," *Ottawa Citizen*, Sept. 27, 2021.

Ezra Levant, "Canadian Military Conducted a Psy-op Against Canadians – What This Means for Freedom," *Rebel News*, Sept. 27, 2021.

Eva Bartlett, "It's Utterly Unacceptable that Canada's Military Ran a Secret Psyops Campaign to Manipulate and Control the Public's Views on Covid," *Russia Today*, Sept. 28, 2021.

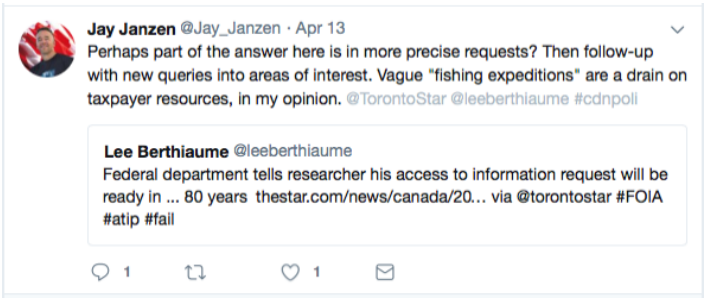
Scott Taylor, "Unpunished Psyops Scheme a Blow to CAF Credibility," *The Hill Times*, Oct. 4, 2021.

Emma Briant, "Canadian Military's Bungled Propaganda Campaigns Should Be a Lesson Across NATO," *Ottawa Citizen*, Oct. 11, 2021.

Hugo Maltais, "New Details Emerge of Canadian Military's Plans to Suppress Popular Opposition Amid COVID-19 Pandemic," World Socialist website, Oct. 21, 2021.

1-1

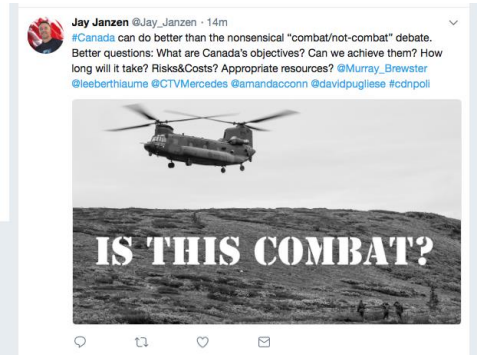
1-2



1-3

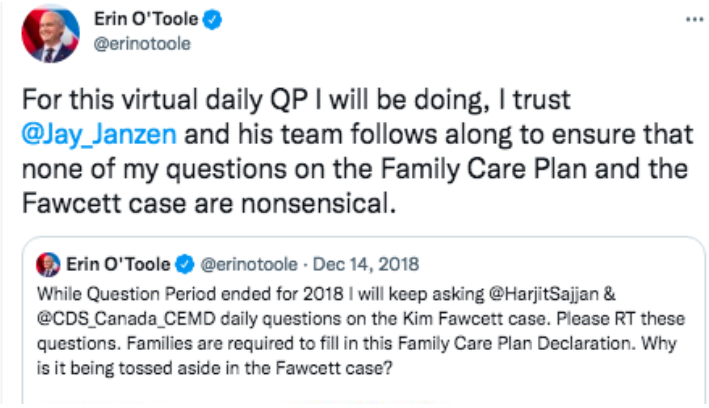
Figure 1

The overt public criticism of media and critics by Col. Jay Janzen, a senior military Public Affairs officer, and actions by others to pressure media organizations to punish some reporters over their coverage about Defence was a deliberate influence strategy that backfired badly. This February 2018 tweet (Fig. 1-1) was a reaction to the "party flight" story that embarrassed senior military leaders and guests travelling on a CAF-sponsored junket to visit troops serving in Greece and Latvia. The officer, appearing in uniform in his profile picture but claiming to be expressing a personal view, prompted discussion inside DND about the appropriate limits for discourse on social media by an identified official. The April 2018 tweet (Fig. 1-2), posted the day the new DND/CAF Joint Information Operations Policy was issued, was little-disguised coercion aimed at the reporter and two of his employers to affect coverage. The April 2018 tweet (Fig. 1-3) was an expression of frustration about use of the *Access to Information Act* to obtain documents at DND. These, plus a fourth tweet the same month about the Mali mission (Fig. 2-1), became known in PA circles as the tweet storm, that in short order through tagging criticized almost every Canadian reporter regularly covering Defence and marked a new low in post-Somalia scandal military-media relations.



2-1

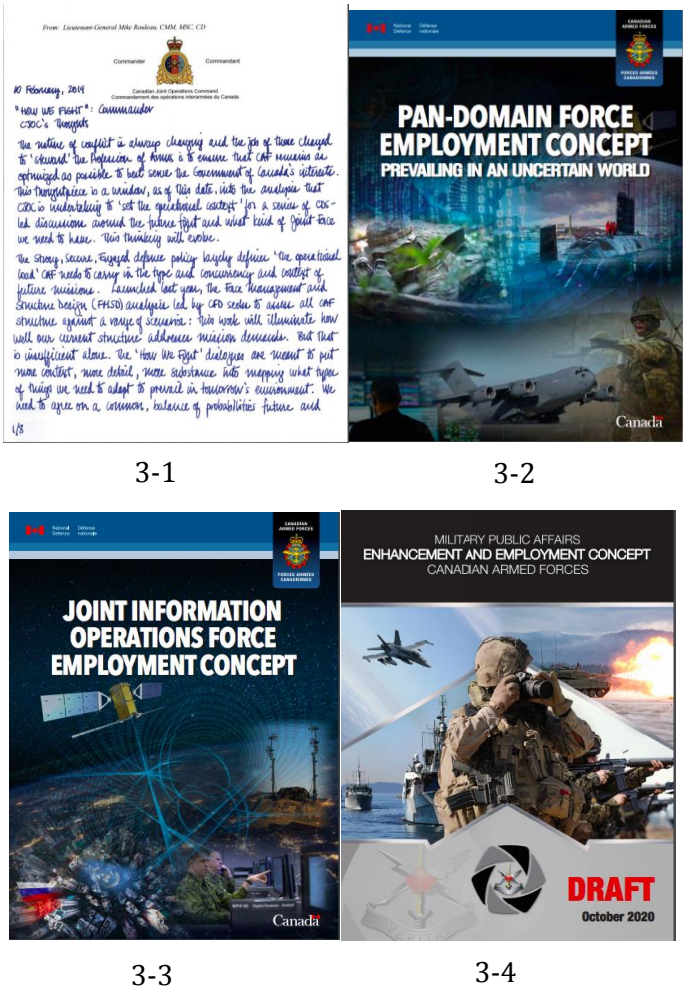
2-2



2-3

Figure 2

In April 2018, Canadian military PAO Col. Jay Janzen tweeted (Fig. 2-1) that the ongoing parliamentary debate and media discussion about the potential for combat during the CAF deployment to Mali was "nonsensical." The commentary led to an angry rebuttal on Twitter by Opposition defence critic James Bezan (Fig. 2-2) and several media articles about the exchange. The criticism, highly unusual for a serving military officer, resonated for months after (Erin O'Toole tweet, Fig. 2-3). In June 2018, in a paper published by the Canadian Forces College, Janzen took umbrage with media about the episode and made the case that "ethical influence" of Canadians rather than "inform" be the operating tenet of Defence Public Affairs. Other tweets around the same time attacking those critical of the military (Fig. 1) suggested this approach was a practical application of "ethical influence" and an example for other leaders and practitioners to follow. Shortly after, the officer was promoted to be director general Military Strategic Communications and received a meritorious service award.



3-1 3-2

3-3 3-4

Figure 3

The use of draft concept papers to progress initiatives and try to change policy without having to first seek formal approval from National Defence Headquarters was a common practice at Canadian Joint Operations Command (CJOC) and the MilStratCom group in ADM(PA). The Gosselin command process review (December 2020) cited these four documents as having moulded staff mindsets about information operations in the CAF. The "How We Fight" paper (Fig. 3-1) by CJOC commander Lt.-Gen. Michael Rouleau was insightful perspective into one dimension of the Defence mandate and set in motion work on various concept policies. These three concept papers (Figs. 3-2, 3-3, 3-4) were designed to appear as if approved, including senior leader forewords, copyright information and the look and feel of a DND publication. In June 2021, the chief of defence staff and the deputy minister determined the documents were "championed by senior CAF leaders as surrogates for obsolete doctrine, yet they have lacked policy cover to ensure alignment with [government] intent and executive leader approval, and have thus been mistaken as authoritative."

4-1

4-2

Figure 4

The MilStratCom initiative drew significant financial resources and full-time staff for long periods including the senior-most PAO (a brigadier-general) and the senior PAO colonel (of just two at that rank) from support to day-to-day Public Affairs activities and long-term planning. This diversion of executive leadership, personnel and focus at a time of high tempo was felt throughout the enterprise, including at Canadian Joint Operations Command, responsible to oversee all international and domestic CAF deployments, including directing the COVID-19 pandemic operation. The net result meant DND/CAF Public Affairs had less capacity to effectively advise leaders, do information campaign planning, engage media and create content to explain the broad range of Defence activities to Canadians (such as the initial effort to mark the Afghanistan monument dedication in May 2019: Fig. 4-1). This also affected the quality of advice in support of relentless ongoing missions and operational demands (Fig. 4-2, the initial public communication following the crash of a RCAF Cyclone helicopter in April 2020).

UNCLASSIFIED (For Official Use Only)

Annex C
To Canadian Armed Forces Military Strategic Communication and Public Affairs
Operationalisation Force Development Plan

CAF Guide to the Employment of Information Activities

Note: These guidelines are intended to provide a general understanding of the approximate authorities that will normally be required when employing information-related capabilities during CAF activities and operations. This is not a standing list of authorities. While some of the required authorities already exist for specific situations, a number of other circumstances will require that authority be sought, occasionally at the highest level. For these reasons, formal authority must always be obtained prior to the employment of information-related capabilities.

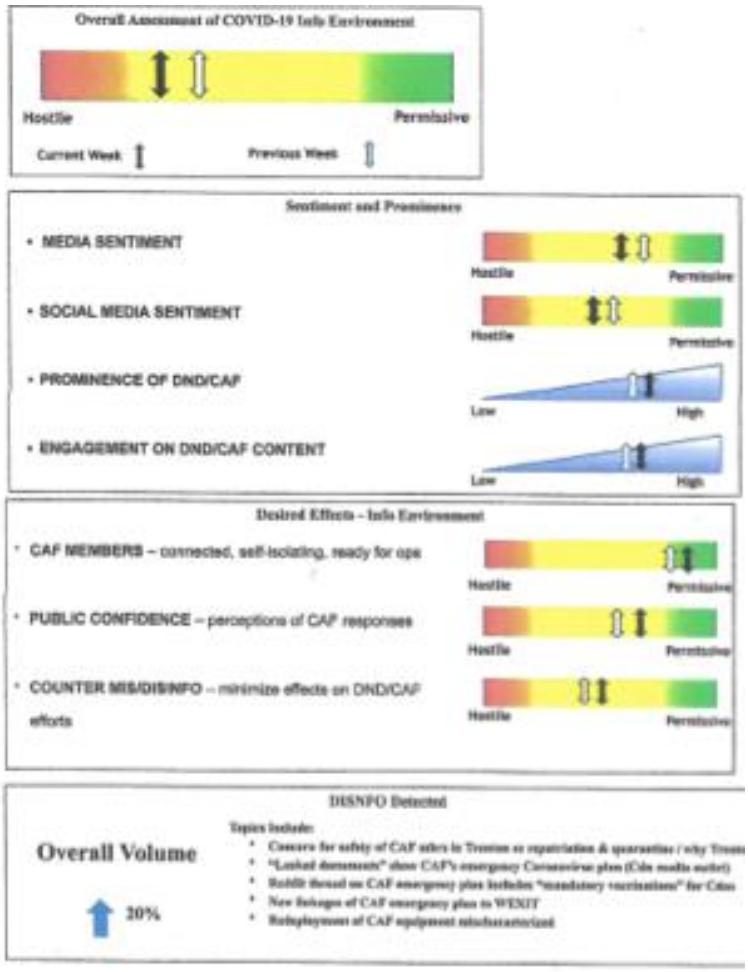
Activity	Intended Audience	Subject Matter	Possible Authority Level
Military PA products	Canadians / Allies	Routine	L3 / L4
Military PA products	Canadians / Allies	Sensitive	L0 / L1
Military PA products	Neutral in-theatre	Routine	L3 / L4
Military PA products	Neutral in-theatre	Sensitive	L2 / TF Comd
Military PA products	Potential Adversaries	Routine	L2 / TF Comd
Military PA products	Potential Adversaries	Sensitive	L0 / L1
CIMIC Products	Canadians / Allies	Routine	L3 / L4
CIMIC Products	Canadians / Allies	Sensitive	L0 / L1
CIMIC Products	Neutral in-theatre	Routine	L3 / L4
CIMIC Products	Neutral in-theatre	Sensitive	L2 / TF Comd
CIMIC Products	Potential Adversaries	Routine	L2 / TF Comd
CIMIC Products	Potential Adversaries	Sensitive	L0 / L1
PsyOps Products	Neutral in-theatre	Routine	L3 / L4
PsyOps Products	Neutral in-theatre	Sensitive	L2 / TF Comd
PsyOps Products	Potential Adversaries	Routine	L3 / L4 or higher
PsyOps Products	Potential Adversaries	Sensitive	L1 / L2 or higher
Info ops Plans	Neutral in-theatre	Routine	L3 / L4
Info ops Plans	Neutral in-theatre	Sensitive	L2 / TF Comd
Info ops Plans	Potential Adversaries	Routine	L3 / L4 or higher
Info ops Plans	Potential Adversaries	Sensitive	L1 / L2 or higher

5-1

Figure 5

Some draft products produced and circulated by the MilStratCom team based in ADM(PA) caused real concern among practitioners. This authorities chart (Fig. 5-1), while never approved or issued, was an effort in spring 2019 to set out when information-related capabilities could be employed, including in Canada, and who could authorize their use. In the previous draft of this document, the use of PSYOPS, military deception and "other capabilities" against Canadians and allies for both "routine" and "sensitive" occasions was included, then removed following critical feedback. Military counter-intelligence investigations of right-wing extremists in the CAF and Communications Security Establishment support to the RCMP are two examples when military information-related capabilities against Canadians could be authorized. The work to define all the possible circumstances of use was led by uniformed PAOs serving in the Public Affairs group and still actively involved in Public Affairs. This suggested National Defence was considering the use of deception, IO and PSYOPS in domestic public communications, which if true, would ruin organizational credibility and institutional reputation.

The reference to "Crown" in the "required authority level" column of Fig. 5-1 means a cabinet minister would normally need to approve the listed activity (L0 = CDS/DM-level approval is required; L1 = assistant deputy minister level or military equivalent; L2 = director general; L3 = director level; L4 = section head level). The use of terminology like PSYOPS and military deception in a domestic context illustrated the MilStratCom initiative mindset and the insufficient distinction in policy and practice between contested overseas operations and domestic activities.



5-2

The draft COVID-19 information environment assessment product (Fig. 5-2), meant to inform commanders, chose as labels "hostile" through "permissive" to describe the degree of public confidence in the CAF and how media were reporting about the military. Not marking "draft" on many products lent them the air of being approved and was an influence activity in its own right. As the CDS and DM acknowledged in June 2021, "it is clear that the development of the various information related capabilities have suffered from a lack of institution-wide strategic level direction and guidance … that is … governed by appropriate authorities and oversight."

6-1 6-2

Figure 6

On Nov. 2, 2020, the *Ottawa Citizen* ran the front-page headline "Canadian Military Wants to Establish New Organization to Use Propaganda and Other Techniques to Influence Canadians." The "weaponization of Public Affairs" characterization, more than five years old, still had resonance (Fig. 6-1). Three days later, then-chief of the defence staff Gen. Jonathan Vance shuttered the project. A week later, he and then-deputy minister Jody Thomas issued DND/CAF-wide guidance to reset the various information-related capability initiatives. In June 2021, acting CDS Lt.-Gen. Wayne Eyre and the DM declared that the initiative and the associated concept paper were "incompatible" with government communications policy and the DND/CAF vision, mission and principles of Public Affairs.

Media coverage of missteps including the IO annex, "fake wolves" and target audience analysis training, left unexplained by MilStratCom practitioners over the course of the initiative's life, damaged National Defence's reputation and provided ample fodder to fuel conspiracies about government and DND/CAF intentions (Fig. 6-2). Insufficient senior military/civilian oversight of a key *Strong, Secure, Engaged* defence policy initiative to improve information-related capabilities was ultimately a failure of DND/CAF leadership and a case of practitioner hubris and communications malpractice.

Acronyms

ADM(PA)	Assistant Deputy Minister (Public Affairs)
CDS	Chief of the Defence Staff
CJOC	Canadian Joint Operations Command
DGPA	Director General Public Affairs
DM	Deputy Minister
IA	Influence Activities
IO/Info Ops	Information Operations
IRC	Information-Related Capabilities
JOIFEC	Joint Information Operations Force Employment Concept
MilPA	Military Public Affairs
MilStratCom	Military Strategic Communications
MPAEEC	Military Public Affairs Enhancement and Employment Concept
PAO	Public Affairs Officer
PFEC	Pan-Domain Force Employment Concept
PSYOPS	Psychological Operations

Author's Note and Acknowledgements

Objective self-introspection is not National Defence's strong suit. Practitioner communities, sub-cultures and leaders under scrutiny for actions and decisions that lead to public missteps generally of their own accord do not actively seek to discover lessons learned. The escape default is to claim a desire to "look forward, not in the mirror" and call for more resources and more training. This approach misses an important point, of course. Identifying the underlying reasons for suboptimal outcomes from necessary initiatives and then fixing the issue(s) reduces risk and the likelihood that events will repeat themselves, thereby increasing the prospect of success the next time around.

This monograph is my take on events central to the MilStratCom initiative, circa summer 2015 to June 2021, from the perspectives of a communications practitioner, outside observer and for a brief period, inside advisor. In late fall 2019, 10 years after retiring from the regular force, I agreed to join the army reserve for a short stint to help try to unstick the stalled DND/CAF's strategic communication reform effort and worked in the Chief of the Defence Staff Initiatives Group for 18 months. Much of this period coincided with the COVID-19 pandemic but was also a time of significant developments in PA and the MilStratCom initiative. I hope this contribution informs any lessons-learned effort and possibly be a primer for ideas about how to make Defence communications and the communications function government-wide more fit for the demands of the current fast-evolving information environment.

My interest in writing about the subject stems mainly from the remarkable acknowledgment by the CDS and DM in June 2021 of the lack of institution-wide, strategic-level direction and guidance over several years to ensure appropriate oversight of activities in the field of communications reform. That, and the declaration that the MilStratCom initiative and related military Public Affairs concept document were incompatible with government policy and the Defence Public Affairs mission, vision and principles suggested a number of questions that deserve answers: What happened? How and why did this happen? In what ways was the effort incompatible? Is anyone accountable for what happened? Who takes this important work forward now? Have the strategy and approach changed to avoid a repeat occurrence or is everyone just doing the same thing as before?

This research is the outcome of several dozen interviews and exchanges with practitioners intimately familiar with the initiative as well as senior officials and officers both serving and retired who willingly shared their views, feedback and observations about the subject. These highly skilled ethical leaders and practitioners have deep experience in the DND/CAF, in coalition operations, at static and deployed NATO HQs, the federal government and in the corporate sector. Understandably, those still serving or recently retired were not comfortable being publicly identified. I am grateful to all those who shared their insights and experiences, including why their concerns when raised were not heard, and why their advice was not taken. Media familiar with the DND/CAF also provided valuable insight about their experiences dealing with the organization.

This is a "tell a lot," not a "tell all" effort. The media have already covered many aspects, incidents, elements and themes of the subject of this monograph. Much important insight is now available via documents obtained or that will be released under the *Access to Information and Privacy Act* (ATIP). None of the content of this monograph stems from classified information. Soon after cancelling the MilStratCom initiative, senior DND/CAF leadership expressed quite pointed views

of what transpired and how events came to pass. This report seeks to unpack and explain their own assessments, connecting the aggregation of developments to a timeline informed by context and perspective from many involved practitioners to explain why leaders came to the conclusions they did. Any errors or omissions in this monograph are mine alone.

This problem set is not going away. Building sustainable communications capability and capacity to successfully compete in the information environment is a truly demanding undertaking and an urgent operational imperative – DND/CAF, the nation and NATO (!) cannot afford a repeat performance of the MilStratCom initiative strategy, approach and tactics.

This monograph is dedicated to serving and retired Canadian PAOs living with moral injuries stemming from demanding, often unheralded long service in frenetic, high-stakes, high-stress environments. Often, their voice is the only frank, unfettered advice to senior leaders making decisions when error or even nuance has serious consequences, including to the credibility and operational effectiveness of the DND/CAF. These practitioners deserve respect and better treatment than they are now receiving from the institution.

About the Author

Brett Boudreau *served in the Canadian Armed Forces for nearly 30 years including 22 years as a Public Affairs officer, with four assignments as a colonel at National Defence HQ, NATO HQ Brussels, the Privy Council Office (Afghanistan Task Force) and most recently, in the army reserve with the chief of the defence staff's office.*

He has worked at NATO HQs in Mons, Brussels and Kabul, is a graduate of the NATO Defence College senior course and holds an Honours BA in political science (Western), and a master of arts degree in public administration (Carleton).

In 2016, the NATO Strategic Communications Centre of Excellence published his book, We Have Met the Enemy and He is Us*, tracing the evolution of StratCom through the lens of the NATO International Security Assistance Force. In 2022, his chapter, "NATO Information Campaigns in Afghanistan 2003-2021," focused on the Resolute Support Mission, was published in the book,* Information Operations From World War 1 to the Twitter Era.

Boudreau has been principal consultant at Veritas Strategic Communications for 12 years and is a Fellow with the Canadian Global Affairs Institute.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.