CAJ
The Canadian Army Journal

NATO ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE POUR L'OTAN

Cutting through the Haze: Grey Zone Operations and Contemporary Threats

Summer 2023

Cutting through the Haze: Gray Zone Operations and Contemporary Threats

Volume Editors

Christopher Maternowski
Aditi Malhotra

Volume Design

Christopher Maternowski

CAJ
The Canadian Army Journal

NATO ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE POUR L'OTAN

Disclaimers

Opinions expressed in the articles remain those of the author and do not represent Government of Canada, departmental or Canadian Armed Forces official policy. The doctrine, training, and other updates do not represent authority for action on that particular topic.

The views and opinions expressed in this publication are those of the contributing authors and do not necessarily represent those of the NATO Association of Canada.

Image Credits

Front cover: "Members from 2e Battalion, Royal 22e Régiment prepare to jump into a trench during RIMPAC 2016 at Camp Pendleton in San Diego, California on July 31, 2016, " July 31, 2016, by Sgt Marc-André Gaudreault, Valcartier Imaging Section, VL08-2016-0020-211.

Back cover: "Members of the Battalion, Royal 22e Régiment, conduct urban combat manoeuvres during exercise SPARTIATE KRUPTO in the training areas of 2nd Canadian Division Support Base Valcartier (QC), on 24 March 2022," March 24, 2022, by Corporal Marc-André Leclerc, Valcartier Imaging Section, Canadian Armed Forces."

All images courtesy of Canadian Armed Forces Combat Camera.

Copyright

CAJ
The Canadian Army Journal

About Us

First established in 1947, the **Canadian Army Journal** (CAJ) is an official publication of the Canadian Army. CAJ is a peer-reviewed journal of ideas and issues, dedicated to professional thought and informed debate on the art and science of land warfare. The CAJ mandate is to promote the discussion of modern land warfare concepts as well as contemporary defence and security issues relevant to the land environment. CAJ also includes articles on broader military subjects including leadership, ethics, military culture, technology and military history.

The Canadian Army Journal
c/o the Editor at the Canadian Army Detachment Kingston
(Canadian Army Land Warfare Centre)
P.O. Box 17000 Stn Forces, Kingston, Ontario, K7K 7B4
Canada
613-540-8713
thearmyjournal@forces.gc.ca

The NATO Association of Canada is an independent, charitable non-profit, non-governmental organization dedicated to the idea that the transatlantic relationship between Canada, the United States, and the nations of Europe is of critical military, economic, and cultural importance to Canadians. The Association's mandate is to promote a broader and deeper understanding of international peace and security issues relating to NATO.

The NATO Association of Canada
48 Yonge Street, Suite 610
Toronto, ON, M5E 1G6
Canada
416-979-1875
info@natoassociation.ca

Contents

1-8
Introduction

Christopher Maternowski and Aditi Malhotra

9-19
Close Engagement in the Gray Zone: Challenges and Opportunities

Peter Gizewski and Nancy Teeple

20-31
Army Sustainment in the Gray Zone: Emergent Technologies as a Double-Edged Sword

Yazan Qasrawi, Peter Gizewski, Abdeslem Boukhtouta, Peter Dobias, and Michael A. Rostek

32-42
Narrative as a Force Multiplier in the Information Battlefield

Suzanne Waldman

43-50
Maintenance Operating Periods in Multi-Domain Operations

Lieutenant Colonel Andrew Bellocchio

51-59
Investigation of Ground-Based Air Defence System Options Using Simulation and Data Farming

Maude Amyot-Bourgeois, George Nikolakakos, and Lynne Serré

60-71
GIS Analysis of Potential Missile Targets in Canada Maximizing Potential Damage

Geoff Pond, Emilie Breuvart, Andrew B. Godefroy, and Cindy Lin

Acknowledgements

The editors would like to acknowledge those who helped to make this inaugural collaboration between the *Canadian Army Journal* (CAJ) and the NATO Association of Canada a reality. To begin, the editors would like to thank the authors for their contributions. The editors also wish to express their gratitude to Brigadier-General André Demers, Colonel Jim Smith, Lieutenant-Colonel Alain Carrier, Major John Bosso, and Dr. Peter Dobias, all of whom contributed considerably to the realization of this publication. Additionally, the editors would like to thank Robert Baines for actively encouraging this volume.

Introduction

Christopher Maternowski and Aditi Malhotra

The sheer range of threats in the contemporary security environment exerts pressure on and tests Western defence establishments, including Canada, the US, and NATO. In addition to the threat of non-state actors, which topped defence agendas in the 2000s, supranational challenges like climate change have entered the scene, sophisticated technologies have become weaponized, and great-power competition and inter-state rivalries have re-emerged.[1] This competition between states plays out in a host of venues and assumes different guises of varying intensity. The Russian invasion of Ukraine, a large-scale, open military confrontation, stands at one end of this force spectrum.[2] On the other sits an array of relatively ambiguous non-traditional warfare tactics or non-military means—instances of foreign meddling in elections and cyber and information operations or disinformation campaigns designed to destabilize Western democracies. While observers can readily perceive open confrontation, recognizing, grasping, and responding to the spectrum of activities that stop short of overt war remains decidedly more difficult.[3]

The spectrum of activities described above informs and guides this volume, which originated from a cross-border initiative, the "25th Annual Canada-US Army Operational Research Symposium" (October 18-21, 2021), focused on the "grey zone," a term that encompasses the various operations that unfold "in the dangerous 'grey' area between peace and war."[4] Delving deeper into the subject, each of the six papers in this volume—a sampling of the symposium—addresses a particular issue within the broader debate on this spectrum of activities, especially grey zone operations or warfare.[5] This edition explores the "murky in-between" of the grey zone.[6] It further establishes that the grey zone will be an agenda-setting—if not messy and contentious—issue for policymakers on both sides of the border—and for the larger NATO alliance—in the years ahead.[7]

Indeed, the shadowy grey zone has provoked debate, including on how to define this notoriously slippery term.[8] The contributions that follow help to give shape and specificity to the hazy contours of grey zone activities. However, for the sake of conceptual clarity, this introduction broadly understands a grey zone operation as an "activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war."[9] An intrinsically capacious concept, states wage grey zone operations in multiple dimensions and domains that span land, air, maritime, space, cyberspace, information, political, economic, and cognitive realms.[10]

The nature of grey zone operations, especially its breadth and conceptual fuzziness, calls into question the conventional understanding of the "spectrum of conflict" that had previously dominated security studies literature.[11] In brief, the spectrum of conflict is a conceptual framework that aims to capture the magnitude and level of violence "ranging from peaceful interaction among international actors (states, corporations, international organizations, non-governmental organizations, etc.) to major combat operations/general war."[12] The spectrum of conflict has traditionally advanced a "linear" interpretation of graduating intensity, with an intermediary "grey zone" existing between the diametrically opposed poles of war and peace.[13] Linear interpretations of conflict that situate the "grey zone" on a rigid spectrum have drawn criticism for, among other reasons, upholding an artificial war-peace dichotomy or even fundamentally misrepresenting the "dialectical" relationship between the two.[14]

The search for alternative frameworks, however, has proved no less fraught.[15] Any competing theory must account for the fact that today's threats are multi-sided and interpenetrating. Furthermore, in this dynamic and ambiguous threat environment, disentangling the "military and nonmilitary means" through which states pursue their goals becomes trying—both can constitute and serve as vehicles for hostile actions that approach or cross "red lines."[16] Nevertheless, in a bid to transcend these perceived limitations of linearity, experts have proposed alternatives, such as a "quadrant" schema with a bisecting vertical and horizontal line that "highlights how actions in one area are connected to activities in another."[17]

To expound, while some experts have called for a "comprehensive approach" to the spectrum of conflict, others have proposed expanded frameworks, namely, the "full spectrum of conflict design" and "contemporary spectrum of conflict."[18] These debates may obscure important common ground. Still, regardless of the variations among these conceptual frameworks, they all intend to problematize and destabilize the contrived demarcation between peace and war. As one commentator notes, "the line between the two has been blurred to the point that they are no longer distinct."[19]

This primer on the grey zone and the spectrum of conflict provides the necessary context for this volume's articles, which illuminate the nature of the threat for Canada, the US, and their NATO allies and partners. Notwithstanding the ongoing debate on the semantics of the grey zone and its proper placement within the spectrum of conflict, scholars and practitioners alike can ill afford to ignore the overall impact of grey zone operations (or warfare) or activities. Russia, China, North Korea, and Iran have seized on grey zone tactics to advance their national interests while minimizing the risk of a major escalation.[20]

Adversarial but non-kinetic actions seek to alter incrementally the post-war order that Western institutions such as NATO help to uphold.[21] Therefore, the West's attention to grey zone warfare is crucial to safeguard its defining structure, security, values, norms, and interests in an increasingly complex and interconnected global landscape. Effective management of the challenges in the grey zone may also prevent escalation into a full-blown conflict or war, further ensuring regional and global stability and security.[22]

As Canada, the US, and their NATO allies and partners face the challenges of dealing with the complexities of the grey zone alongside more conventional operations, planners and decision-makers have continued to work toward finding increasingly effective ways to address them. Innovation—a subject of heightened interest across Western defence establishments, as NATO's investments in emerging and disruptive technologies (EDTs) and Defence Innovation Acceleration for the North Atlantic (DIANA) evidence—offers one way of doing so.[23] Defence innovation appears prominently in this volume and helps link the six articles that follow. Each of the contributions in this volume establishes that tackling the grey zone, notably its "amorphous and ever-changing character," and other arenas of competition requires continuous innovation—technological and otherwise.[24]

Like the grey zone, "military innovation" has definitional dilemmas.[25] Yet, although definitions abound, "change" remains a widely accepted and core feature of prevailing understandings.[26] As Barry Scott, Nalauhai Kaahaaina, and Christopher Stock assert: "Overall, innovation is about change. Innovation in the military is about staying ahead of the pace of change in comparison to an opposing force."[27] Innovation, though, often has marked technological connotations, which many definitions reflect.[28] According to one observer, "generally the first thing that comes to mind is product innovation using technology."[29]

Despite its emphasis on and association with developing cutting-edge technology, innovation can—and does—assume a multiplicity of forms.[30] It can, for instance, encompass finding

new contexts or creative uses for an extant "capability."[31] Nor must meaningful innovation result in a striking or enduring transformation. On the contrary, even less dramatic and fleeting innovations can make an impact.[32] Questioning the idea of innovations as "silver bullets," James Wirtz summarizes: "Many innovations are modest, unfold at the tactical level of war, and often prove to be only temporarily effective as opponents usually come up with countermeasures in short order."[33] In this vein, the contributions in this volume provide concrete examples of how Canada, the US, and their NATO allies and partners can adapt and exploit extant technologies and systems to gain insights and an overall edge in grey zone activities as well as in conventional operations.

In the volume's introductory and scene-setting paper, **Peter Gizewski** and **Nancy Teeple** expand on the concept of the grey zone. Through the lens of the Canadian Army (CA), the authors assess the "challenges and opportunities" of the grey zone and the measures taken to compete within it. They conclude that the CA remains on track in dealing with the issue. However, to develop a maximally effective and customized response, the CA must continue to innovate by adopting a "whole-of-government approach," as the grey zone poses a "government- and society-wide challenge."

Taking the debate further, the following paper in the volume speaks to the subject of sustainment capacity, a crucial component of military operations that adversarial grey zone activities can compromise. The paper revolves around the current trend of Western militaries leveraging emergent networked technologies to enhance sustainment capabilities. The authors, **Yazan Qasrawi**, **Peter Gizewski**, **Abdeslem Boukhtouta**, **Peter Dobias**, and **Michael A. Rostek**, contend that although technological innovations and advances, particularly networked technologies, have helped to bolster CA's sustainment activities, they have also opened the force to grey zone threats. For the CA to be "operationally effective and efficient in the Future Land Operating Environment," it will need to fashion a "robust sustainment system that integrates into its design defences against grey zone activities."

Addressing the issue of the information environment in grey zone warfare, **Suzanne Waldman** concentrates on virtual spaces, where grey zone operations flourish. In this busy and contested space, Canada is waging "narrative battles" against the falsehoods and disinformation that state and non-state actors disseminate. To succeed, Canada's communicators must assume a proactive stance and offer alternatives. Waldman argues for innovation through the adaptation of pre-existing "narrative frames" that would enable those tasked with communicating the government's message to craft and relay messages that can inform and unseat adversarial narratives, giving Canada an edge in the twenty-first century "information battlefield."

Andrew Bellocchio shifts to the subject of air power, which has applications—reconnaissance missions, transportation, logistical support, and power projection—in the grey zone and beyond.[34] He highlights the need for militaries to undertake "independent manoeuvre" in multi-domain operations. "To achieve independent manoeuvre and function in austere locations," writes Bellocchio, "aviation units must be able to operate for short periods with minimal sustainment (e.g., maintenance)." He focuses on innovation in the US by proposing a rethink of maintenance practices and analyzes the implications of rolling out Future Vertical Lift, defined as "the next generation of rotor craft." Drawing on a 1990s-era innovation from the UK's Royal Air Force, Bellochio makes a case for the US to embrace Limited Maintenance Operating Periods, an adaptation of Maintenance Free Operating Periods.

Maude Amyot-Bourgeois, **George Nikolakakos**, and **Lynne Serré** address the topic of Canada's "capability to protect its land-based force elements and key elements against airborne attacks"—a fixture of contemporary grey zone operations. Using the data-farming process—an existing practice that uses computational experiments—they "assess the performance

of different Ground-Based Air Defence (GBAD) system options against various airborne threats." Through their analyses, the authors offer a detailed and informed understanding of the most effective GBAD system(s) for deployment within the Canadian Armed Forces.

Complementing the theme of innovation with existing technologies, the concluding contribution from **Geoff Pond**, **Emilie Breuvart**, **Andrew B. Godefroy**, and **Cindy Lin** uses existing modelling software in a similarly predictive capacity in the context of airborne threats. With the help of existing data and mapping software, Pond et al. consider the locations that state and non-state actors would most likely target in a possible inter-continental ballistic missile or cruise-missile strike. The authors show how the innovative use of pre-existing resources can help Canada remain prepared for the missile launches that can feature in conventional as well as grey zone operations.[35] In so doing, they provide a salutary reminder that grey zone operations add to rather than supplant traditional threats.

This volume calls attention to the growing salience of grey zone threats within the broader and evolving paradigm of the spectrum of conflict and the pressing need to address them. It also underscores that innovation will continue to play a role across operating domains and in all forms of conflict. However, with the cost of advanced defence assets on an upward trajectory, Western governments could encounter a barrier to funding innovations, especially while balancing the competing priorities enumerated at the outset of this introduction.[36] Under these evolving circumstances, shifting how Canada, the US, and NATO allies approach innovation will be vital for maintaining competitiveness. While EDTs and other cutting-edge technologies will undoubtedly help in this aim, these essays show that Ottawa and Washington can also benefit by innovating with what is already available. This edition outlines some of the possibilities.

This volume, as well as the symposium that inspired it, have facilitated collaboration on several levels. The volume and symposium have brought together members of the defence community within Canada and the US, two long-time allies and founding NATO members. The volume embodies collaboration in another sense: a first-ever joint endeavour between the Canadian Army Journal (CAJ) and the NATO Association of Canada. The CAJ aims "to promote the discussion of modern land warfare concepts as well as contemporary defence and security issues relevant to the land environment."[37] Meanwhile, the NATO Association of Canada seeks "to educate and engage Canadians about NATO and NATO's goal of peace, prosperity and security."[38]

Given these overlapping missions, a natural synergy exists between the CAJ and the NATO Association of Canada. Specifically, both organizations identified shared goals in broadening the Canadian security community and raising awareness of critical issues, including the spectrum of conflict and grey zone operations. This combined effort also affords an opportunity to help bridge the gap between practitioners and the larger public, sparking and sustaining the cross-cutting dialogue so vital to understanding the marked complexities of the contemporary security landscape in which Canada, the US, and NATO allies and partners operate.

Endnotes

[1] On non-state actors and the counterinsurgencies of the 2000s, see Thomas G. Mahnken, Evan B. Montgomery, and Tyler Hacker, "Innovating for Great Power Competition: An Examination of Service and Joint Innovation Efforts," Center for Strategic and Budgetary Assessments, January 11, 2023, https://csbaonline.org/research/publications/innovating-for-great-power-competition-an-examination-of-service-and-joint-innovation-efforts; Mark Pomerleau, "In light of great power competition, DOD reevaluating irregular warfare and info ops," Defense Scoop, November 21, 2022, https://defensescoop.com/2022/11/21/irregular-warfare-and-info-ops-great-power-competition-dod/. On the proliferation of threats and challenges, see "A New Era of Conflict and

Violence," United Nations, last accessed July 9, 2023, https://www.un.org/en/un75/new-era-conflict-and-violence; António Guterres, "'Our World Is in Big Trouble', Secretary-General Warns Assembly, Urging Member States to Work as One United Nations," SG/SM/21466, speech, September 20, 2022, https://press.un.org/en/2022/sgsm21466.doc.htm. On climate change specifically, see Christopher Maternowski, ed., *Navigating a Global Crisis: Climate Change and NATO* (Toronto: NATO Association of Canada, 2023), https://natoassociation.ca/wp-content/2023/02/NAOC-Climate-Change-publications-v2.pdf. On technology in particular, see Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (2020): 91-94, https://tnsr.org/wp-content/uploads/2020/07/06_TNSR-Journal-Vol-3-Issue-3-Hersman.pdf. On great-power competition, see Jeff Goodson, "Irregular warfare in a new era of great-power competition," Modern War Institute, May 20, 2020, https://mwi.westpoint.edu/irregular-warfare-new-era-great-power-competition/.

[2] To be clear, even operations positioned on "the lower end of the spectrum" can, in fact, be intense. For a discussion that problematizes this spectrum in the context of US operations in Afghanistan and Iraq, see Paul Scharre, "Spectrum of What?," *Military Review* 92, no. 6 (November/December 2012): 73-79, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20121231_art012.pdf.

[3] Nora Bensahel, "Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex," February 13, 2017, Foreign Policy Research Institute, https://www.fpri.org/article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex/.

[4] Anthony Robertson, "What is Grey Zone confrontation and why is it important?," The Cove, July 18, 2022, https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important#:~:text=Grey%20zone%20tactics%2C%20confrontation%2C%20and,area%20between%20peace%20and%20war. See, too, Forward Defense experts, "Today's wars are fought in the 'gray zone.'" Here's everything you need to know about it.," Atlantic Council, February 23, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/; Tahir Mahmood Azad, Muhammad Waqas Haider, and Muhammad Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," *World Affairs* 186, no. 1 (Spring 2023): 84-89, https://doi.org/10.1177/00438200221141101. Note that various other terms describe the gray zone." For some of these terms, see Peter Gizewski and Nancy Teeple, "Close Engagement in the Gray Zone: Challenges and Opportunities," in this volume; "Gray Zone Project," Center for Strategic & International Studies (CSIS), last accessed August 14, 2023, https://www.csis.org/programs/gray-zone-project; Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid Warfare—Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (2020): 13, https://digital-commons.usnwc.edu/nwc-revivew/vol73/iss1/4.

[5] On gray zone as a "form of warfare," see Joseph T. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1st Quarter, January 2016): 101-109, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf. For a discussion of "hybrid threats" more broadly, see John Chambers, "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army" (Modern War Institute at West Point, October 18, 2016), https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

[6] Forward Defense experts, "Today's wars are fought in the 'gray zone.'"

[7] Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," 84-88. Nora Bensahel also tentatively forecasted an increase in gray zone activity. See Besahel, "Darker Shades of Gray." For a discussion of the grey zone in the context of Russia and the Eastern Flank, see, for instance, Ben Connable et al, "Russia's Hostile Measures: Combatting Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition" (Santa Monica, CA: RAND Corporation, 2020), https://apps.dtic.mil/sti/pds/AD1090520.pdf.

[8] Robertson, "What is Grey Zone confrontation and why is it important?" See, too, Forward Defense experts, "Today's wars are fought in the 'gray zone.'"; Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," 84-89, 94-95; See Gizewski and Teeple, "Close Engagement in the Gray Zone."

[9] Hal Brands, "Paradoxes of the Gray Zone," https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

[10] Anil Khosla, "Airpower in the grey zone," United Service Institution of India, last accessed August 7, 2023, https://www.usiofindia.org/publication-journal/airpower-in-the-grey-zone.html.

[11] On historical antecedents, see, among others, Michael Fitzsimmons, "The False Allure of Escalation Dominance," War on the Rocks, November 16, 2017, https://warontherocks.com/2017/11/false-allure-escalation-dominance/; Col. John J. Neal, "Defending against nonlinear threats," *per Concordiam* 10, no. 1 (2020), 19, https://perconcordiam.com/perCon_V10N1_ENG.pdf; Hersman, "Wormhole Escalation in the New Nuclear Age," 91-94.

[12] Aurelian Ratiu, "Comprehensive Approach in the full spectrum of conflict," *International Conference Knowledge-Based Organization* 24, no. 1 (2018): 185-191, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjNvonDoMKAAxV5lYkEHaYlCQMQFnoECBQQAQ&url=https%3A%2F%2Fsciendo.com%2Fpdf%2F10.1515%2Fkbo-2018-0027&usg=AOvVaw3Em1igzhlcuBherLowLAm4&opi=89978449.

[13] See Neal, "Defending against nonlinear threats," esp. 19-22. For a critique of intensity, see Scharre, "Spectrum of What?" On quadrants, also see Robert S. Burrell, "A Full Spectrum of Conflict Design: How Doctrine Should Embrace Irregular Warfare," Irregular Warfare Initiative, March 14, 2023, https://irregularwarfare.org/articles/a-full-spectrum-of-conflict-design-how-doctrine-should-embrace-irregular-warfare/.

[14] On the evolution of thinking, see Neal, "Defending against nonlinear threats," esp. 19-22; Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018): 30–47, https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/. For an overview of criticisms of the gray zone, see Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," 94-95; Brands, "Paradoxes of the Gray Zone." For a particularly critical perspective of the gray zone, see Stoker and Whiteside, "Blurred Lines:," 12-48, esp. 17, https://digital-commons.usnwc.edu/nwc-revivew/vol73/iss1/4.

[15] On alternative frameworks, see Heather M. Bothwell, "Gray Is the New Black: A Framework to Counter Gray Zone Conflicts," *Joint Force Quarterly* 101 (2021): 25-30, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2556217/gray-is-the-new-black-a-framework-to-counter-gray-zone-conflicts/; Miroslaw Banasik, "Unconventional War and Warfare in the Gray Zone. The New Spectrum of Modern Conflicts," *Journal of Defense Resources Management* 7, no. 12 (2016): 37-46, https://doaj.org/article/dffd2b6f4cdf4c159ab1dc444cbb138e; Hoffman, "Examining Complex Forms of Conflict," esp. 34-36, https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

[16] Neal, "Defending against nonlinear threats," 17, 21.

[17] See Neal, "Defending against nonlinear threats." On quadrants, also see Burrell, "A Full Spectrum of Conflict Design."

[18] Aurelian Ratiu, "Comprehensive Approach in the full spectrum of conflict,"; Burrell, "A Full Spectrum of Conflict Design."

[19] Neal, "Defending against nonlinear threats," 20.

[20] See Gizewski and Teeple, "Close Engagement in the Gray Zone." Also see, Kathleen Hicks, "Russia in the Gray Zone," Aspen Institute, July 19, 2019, https://www.aspeninstitute.org/blog-posts/russia-in-the-gray-zone/; "Russia's Prigozhin admits interfering in U.S. elections," *Reuters*, November 7, 2022, https://www.reuters.com/world/us/russias-prigozhin-admits-interfering-us-elections-2022-11-07/#:~:text=LONDON%2C%20Nov%207%20(Reuters),efforts%20to%20influence%20American%20politics; Daniel R. Russel and Blake H. Berge, *Weaponizing the Belt and Road Initiative* (NY: Asia Society Policy Institute, September 2020), https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf; Chin-Kuei Tsui, "China's Gray Zone Activities and Taiwan's Responses," *The Stimson Center*, December 12, 2022, https://www.stimson.org/2022/chinas-gray-zone-activities-and-taiwans-responses/; Sanghoon Kim, "North Korea Is

Weaponizing the Naval 'Gray Zone' Against the South," *U.S. Department of Defense Non-lethal Weapon Program*, October 2, 2021, https://jnlwp.defense.gov/Media/News/Article/2815408/north-korea-is-weaponizing-the-naval-gray-zone-against-the-south/; Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of Its Asymmetric Way of War," *The Washington Institute for Near East Policy*, March 19, 2021, https://www.washingtoninstitute.org/policy-analysis/irans-gray-zone-strategy-cornerstone-its-asymmetric-way-war.

[21] For an explanation of "postwar order," see, Michael J. Mazarr, "How to Save the Postwar Order," *Foreign Affairs*, May 6, 2022, https://www.foreignaffairs.com/articles/world/2022-05-06/how-save-postwar-order#:~:text=The%20order%20embodies%20norms%2C%20imperfectly,at%20any%20time%20since%201990. Brands notes this "incremental aggression," noting gray zone operations "eat away at the status quo one nibble at a time." See Brands, "Paradoxes of the Gray Zone," 1. See, too, Gizewski and Teeple, "Close Engagement in the Gray Zone."

[22] Hal Brands, "Paradoxes of the Gray Zone."

[23] On EDTs and DIANA, see "Emerging and disruptive technologies," North Atlantic Treaty Organization, last modified June 22, 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm; Scott Burns, "DIANA: Defence Innovation Accelerator For The North Atlantic," NATO Association of Canada, March 7, 2023, https://natoassociation.ca/diana-defence-innovation-accelerator-for-the-north-atlantic/. Some gray zone-specific innovations in the US include the Defense Advanced Research Projects Agency's "Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS), an AI-informed, "software-based program." See Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," 100-101.

[24] Ashley Mattheis et al., *Blind Sided: A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone* (Arlington, VA: Irregular Warfare Center, February 2023), 18, https://irregularwarfarecenter.org/wp-content/uploads/03142023_Blind_Sided.pdf.

[25] For an overview of the subject, including debates within the literature, see Michael C. Horowitz and Shira Pindyck, "What is a military innovation and why it matters," *Journal of Strategic Studies* 46, no. 1 (2023): 85-114, https://doi.org/10.1080/01402390.2022.2038572. See also Ola Modig and Kent Andersson, "Military Innovation as the Result of Mental Models of Technology," *Scandinavian Journal of Military Studies* 5, no. 1 (2022): 46, https://doi.org/10.31374/sjms.117.

[26] P.M. Picucci et al., "Categorizing Defense Innovation," Defence Acquisition University (DAU), March 9, 2021, https://www.dau.edu/library/defense-atl/blog/Categorizing-Defense-Innovation. Also see, Theresa Chadwick et al, "Characterizing Novelty in the Military Domain," (paper submitted to International Command and Control Research and Technology Symposium, February 2023), https://doi.org/10.48550/arXiv.2302.12314.

[27] Barry Scott, Naluahi Kaahaaina, and Christopher Stock, "Innovation in the Military," *Small Wars Journal*, February 10, 2019, https://smallwarsjournal.com/jrnl/art/innovation-military.

[28] On the contested position of technology within definitions of military innovation, see Horowitz and Pindyck, "What is military innovation and what it matters," esp. 91-93.

[29] Carlos A. Segura Villarreal, "Military Strategy Innovation: Innovating with the support of the Modern Strategic Tool: Strengths, Weaknesses, Opportunities and Threats (SWOT) + 1," *Journal of the Americas, Second Edition 2021*, 186, https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%203%20Issue%202/04-Segura_eng.pdf.

[30] For a survey, see Horowitz and Pindyck, "What is a military innovation and why it matters."

[31] Horowitz and Pindyck note this point and make reference in their outline of "The Military Innovation Process." See Horowitz and Pindyck, "What is a military innovation and why it matters," 86, 88, 95, 100. Reference to "capability" from Picucci et al., "Categorizing Defense Innovation." See, too, Segura Villarreal, "Military Strategy Innovation," 186; Modig and Andersson, "Military Innovation as the Result of Mental Models of Technology," 46.

[32] Horowitz and Pindyck not only observe that "can be small in size and scope," but also suggest "separating the definition of an innovation from its success." See Horowitz and Pindyck, "What is a military innovation and why it matters," 98-99.

[33] James J. Wirtz, "A Strategist's Guide to Disruptive Innovation," *Military Strategy Magazine* 8, no. 4 (Spring 2023): 5, https://www.militarystrategymagazine.com/wp-content/uploads/2023/05/MSM-volume-8-issue-4.pdf.

[34] For context, see Mike Pietrucha and Jeremy Renken, "Blurring the Lines Part III: Airpower Applications in the Gray Zone," War on the Rocks, April 18, 2019, https://warontherocks.com/2019/04/blurring-the-line-part-iii-airpower-applications-in-the-gray-zone/.

[35] On missiles and grey zone operations, see Maude Amyto-Bourgeois, George Nikolakakos, and Lynne Serré, "Investigation of Ground-Based Air Defence System Options Using Simulation and Data Farming," in this volume. For more on Iran's grey zone operations and "toolkit," including its use of missiles, see Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of its Asymmetric Way of War," *PRISM* 9, no. 2 (March 2021): 77-97, esp. 81-86, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-2/prism_9-2.pdf.

[36] On cost, see Marcus Hellyer, "Special Report: Understanding the Price of Military" (Australian Strategic Policy Institute, May 2022), ch. 2, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-05/SR184%20Understanding%20the%20price%20of%20military%20equipment.pdf?VersionId=0UI.LyXt2kUsK2cjYVYdJp8uEnhtajky.

[37] "About the Canadian Army Journal (CAJ)," Government of Canada, last modified April 26, 2023, https://www.canada.ca/en/army/services/canadian-army-journal/about-caj.html.

[38] "About Us," NATO Association of Canada, last accessed August 2, 2023, https://natoassociation.ca/about-us/.

Close Engagement in the Grey Zone: Challenges and Opportunities

Peter Gizewski and Nancy Teeple

Recent years have witnessed a growing willingness and capacity on the part of adversaries to undertake operations in the grey zone to achieve objectives at the West's expense.[1] Indeed, conducting actions below the threshold of war raises the prospect of avoiding Western military strengths while simultaneously achieving one's goals with a lower risk of reprisal. Such operations—conducted in multiple domains, blurring the boundary between peace and war—represent an increasingly salient challenge for Western armies, including the Canadian Army (CA).

To what extent are Western militaries moving to meet the challenge? This paper examines the question from a CA perspective. More specifically, it assesses how the CA is moving to meet the challenge by examining *Close Engagement: Land Power in an Age of Uncertainty*, "the capstone operating concept designed to guide the development of Canadian land forces for the next 10 to 15 years."[2] Close Engagement is defined as "the ability to conduct both lethal and non-lethal activities at the tactical level to create effects that have influence across the physical, moral and cognitive planes within the operating environment."[3]

Following a brief description of the nature and characteristics of grey zone conflicts, this article assesses the degree to which Close Engagement serves to provide the tools required to address the challenges that the grey zone presents. It notes that while the concept offers several initiatives that move the army in the right direction, much remains to be done, particularly in operationalizing the concepts and providing a coherent and effective doctrinal framework that addresses how the army should operate in a manner that meets grey zone challenges. This work underlines that the grey zone challenge transcends not only the army, but also the Canadian Armed Forces (CAF). Developing effective responses to these contemporary challenges must be a comprehensive and government-wide effort.

Defining the Grey Zone and the Growing Use of Grey Zone Activity

Defining grey zone activities is challenged by the "lack of a universal definition under international law," with the term originating in military and policy discussion, and further complicated by the interchangeable use of the terms "sub-threshold warfare," "hybrid warfare," "measures short of armed conflict," and "measures short of war." This ambiguity has worked to ensure that no clear set of protocols exists for addressing such activities under the international Law of Armed Conflict (LOAC). Nevertheless, Elizabeth Kiessling asserts that "a majority of scholars and practitioners seem to agree that grey zone activities share a unifying characteristic, with states undertaking such actions "to gain a strategic advantage while remaining below the level that would trigger a military response."[4] A RAND Corporation study defines grey zone as "an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution for events."[5] Thus, we can understand grey zone activity as aggressive—but not necessarily violent—actions below the threshold of armed conflict.

Such activities seek to avoid a conventional response and retaliation, which makes it difficult for the defending state to enforce red lines that an adversary approaches but does not cross.

Grey zone actors can asymmetrically target the vulnerabilities of a superior military force and economic entity using methods that are cost-effective, efficient, and eliminate attribution. This means achieving objectives without triggering a conflict, which would be perceived on a global scale as an out-of-proportion (and likely unjustified) response. For adversaries, exploiting the grey zone provides an effective means to support expansion and claim territory, undermine the Western liberal order, create political divisions among Western allies and partners, and foster increasing uncertainty.

Great-power adversaries, such as Russia and China, are already operating in the grey zone to undermine the international rules-based order, and take advantage of opportunities to exploit divisions within civil society to change borders and expand influence and territory.[6] In addition, non-state actors operate in the grey zone, using low-cost technologies to achieve strategic effects and take risks at low costs against superior Western forces, particularly if they can avoid attribution in various domains (especially cyber).[7] Actors are thus motivated to use grey zone methods based on a favourable risk calculus, with the benefits of such actions outweighing the likely costs.

Key Characteristics of Grey Zone Activity

Grey zone activities pose challenges to Western forces in terms of detection, attribution, and proportional response. The *NATO Warfighting Capstone Concept* (NWCC) indicates that adversaries are using increasingly sophisticated strategies coordinated through political, military, economic, and information efforts that are executed via the application of new technologies and capabilities. The multidimensional battlespace of the grey zone involves the new domains of cyber, space, and information, alongside the traditional domains of land, sea, and air. Complexity is introduced by the combined physical, virtual, and cognitive realms, the physical and non-physical space, and simultaneous actions rather than linear and binary.[8] Throughout, the strategic and tactical boundaries are often blurred.

Grey zone activities can be wide ranging and can include, *inter alia*, attempts to interfere in state elections and political processes through the use of cyber operations aimed at information manipulation and the creation of political divisions, the use of proxies to engage in attacks on state territories, infrastructure, and political figures, the use of electromagnetic weapons to obstruct government and military communication systems, and cyber-attacks on critical utilities and infrastructure.[9] While generally tactical in character, their use can provide the means to achieve strategic ends, with the response by the affected party dependent on context. As a result, addressing the challenges posed by such activities must be determined on a case-by-case basis.

As noted above, real-world examples are numerous. Russia's use of "little green men" in Crimea and its interference in the 2016 US presidential elections are exemplary instances. In the case of the former, Moscow's use of personnel lacking identifying insignia to support insurgent forces in Ukraine aided in the successful annexation of Crimea, without Russia going to war.[10] As for the latter, grey zone activity included the use of coercive cyber operations aimed at manipulating the electoral process in a manner intended to favour Moscow's preferred candidate in the election.[11]

China's island-building activities in the South China Sea offer yet another example. Chinese actions are increasingly leading to the creation of approximately 3,200 acres of new land within the region and a string of outposts—some highly militarized—that have increased Beijing's capacity to control the South China Sea in all scenarios short of war with the US.[12] Meanwhile, its Belt and

Road Initiative (BRI) has provided a ready means for leveraging Beijing's economic might to shape other countries' interests and to "deter confrontation or criticism of China's approach to or stance on sensitive issues." In fact, some speculate that the BRI's "debt-trap diplomacy" creates opportunities for China to enable their military forces to establish beachheads in those nations.[13] Such activities are not solely confined to the great powers—a fact illustrated by North Korean cyber-attacks on businesses such as Sony and Iran's support of militant groups that provoke enemy forces while Tehran maintains plausible deniability.[14] Undoubtedly, Iran engages in information operations aimed at projecting its image as a regional powerhouse, conducts cyber-attacks and cyber espionage against regional rivals (e.g., Saudi Arabia and Israel), and jams satellite communication broadcasts from Western nations such as the UK and the US.[15] The following table lists the range of grey zone activities in which adversaries have achieved varying levels of success and deniability.

Activity	**Method/Examples of Execution**
Information/Disinformation attacks	Foreign election interference or false text message/email scams: • Campaigns to discredit opponents/ subversion/creation of internal political divisions[16] • Cyber interference, as well as cognitive manipulation, against the domestic population of a state. These actions include hacking the emails of candidates to reveal personal information publicly or disseminating disinformation to discredit a candidate
Use of proxy forces	Use of proxy actors to enhance deniability: • Proxy attacks on cities or infrastructure • Use of special forces or mercenaries to foment resistance in contested territories • Use of criminal entities to assassinate (or attempt to assassinate) dissidents or state leaders
Economic coercion	• Adversary purchasing and disabling a piece of infrastructure such as an oil refinery • Adversary investment in infrastructure within countries experiencing economic setbacks, thereby creating conditions for potential coercion by the investor[17]

Territorial encroachment	• Seizing fishing lanes or sovereign territory. This method may include the manipulation of international law
Cyber operations	• Espionage involving the theft of intellectual property for economic advantage, or the theft of personal information about customers/employees/operatives (this can include Artificial Intelligence [AI] spoofing) • Disruption and disabling operations used against networked infrastructure and communications • A cyber-attack on utilities or drones attacking an airport
Electromagnetic attacks	• Use of electromagnetic weapons against communications and diplomats (assumed to be off limits)

Table 1: Grey Zone Activities[18]
Source: Drawn from Morris et al., *Gaining Competitive Advantage*, 8-12.

Close Engagement in the Grey Zone

Addressing such threats requires recognition and response to several key realities in the security and operational environments. In particular, it requires recognition that conflict is increasingly multidimensional, and that it can and will involve capabilities that extend far beyond those traditionally or primarily associated with the conduct of warfare. It is equally crucial to understand that those involved in the conduct of grey zone warfare may not wear a military uniform, and that warfare itself and the strategies and tactics employed to prosecute it need not necessarily be kinetic in character. Nor, for that matter, will conflict and its prosecution necessarily be confined to a particular territorial location or have a clear beginning or end.

Accordingly, this calls for an approach that eschews simple binary and linear conceptions of peace and war. It requires an approach that recognizes the need for a wide range of capabilities, skill sets, and actions—many of which can be effectively applied below the level of armed conflict, including capacities to adapt, monitor, collect, and analyze information quickly and accurately, and to respond effectively within impacted theatres of operation and beyond them. Moreover, it demands an approach capable of harnessing a wide array of elements of national power—material and human—to address promptly the challenges that may arise.

Close Engagement: Canada's Army in an Age of Uncertainty provides an operating concept that offers a few elements particularly well suited to meet challenges in the grey zone.[19] The concept is explicit in its recognition that the prosecution of conflict need not be kinetic to generate significant impacts. It is also clear in its understanding of the need for a range of skill sets and cross-governmental cooperation for effectively addressing threats. The concept underlines the importance of "organizing, equipping, training, and employing Canadian land forces within an

integrated CAF joint force," as well as practicing a comprehensive, whole-of-government approach to operations involving military, interagency, multinational, and public partners.[20]

As for the army itself, the concept stresses the need for greater promotion of historical and cultural understanding and knowledge in the education and training of personnel, intelligence gathering, influence activities, media operations, and personal engagement in the conduct of land combat.[21] Indeed, such capabilities are essential for developing and promoting effective counters to grey zone threats, including building capacity with regional allies, creating strong narratives capable of winning support for operations being planned and/or conducted, and shaping counter-narratives for defeating adversarial efforts to erode the legitimacy of those operations.

Beyond this, the concept underlines the need for systems that allow for safe, secure, and effective coordination and collaboration, and that enhance analytical capability and information security. In this regard, it places a strong emphasis on the development of the following:

- A secure network as the critical backbone of army operations;
- effective and agile Command and Control (C2) support systems;
- increased sensors and information feeds;
- autonomous, persistent surveillance capabilities, along with the processing and analysis capabilities needed to exploit them—an automated-analysis capability to accelerate processing times;
- cyber defences to ensure the safety of information and communications;
- decision aids, such as the development of AI systems to enhance support for decision-making and the planning and execution of operations with greater speed and accuracy (agility); and
- Empowered Combined Action Teams (ECAT)—small in size and capable of rapid dispersion—if and when required (to help ensure a limited footprint and a capacity to blend into and interact with relevant populations on the ground as needed).[22]

To be sure, such capabilities and skill sets are applicable to addressing challenges that span the full spectrum of conflict. That said, the emphasis placed on them in *Close Engagement* demonstrates a marked recognition that the character of warfare—and the capabilities needed to address it—are changing significantly, especially given that many of the challenges likely to confront us remain below the level of conventional warfare (at the lower end of the conflict spectrum).[23]

Operationalizing *Close Engagement* in the Grey Zone

The extent to which such capabilities—once achieved—can be effectively harnessed to counter adversarial challenges in the grey zone remains an open question. On the one hand, such activities *do* represent a growing concern and demand responses. That said, addressing them must be balanced against the fact that preserving the capacity to apply kinetic force represents the chief function of the CAF, including the CA. The capacity to bring hard power to bear and a willingness to do so through multiple means serves to set the limits of grey zone activity. To deter an adversary, one must be able to demonstrate the ability to deny through capabilities that counter and defeat threats.

Beyond this, the CAF and CA's development of effective strategies and responses for addressing grey zone challenges is a work in progress. Many of the capabilities required for addressing such threats, as well as the emphasis placed in *Close Engagement* on obtaining them

(particularly fashioning doctrine aimed at effectively countering them) continue to be insufficient in many respects. For instance, the need to be dispersed and, at the same time, fully networked relies on technological developments not fully developed or integrated with military systems.[24] Interoperability with allies poses additional challenges, with procedures and protocols that allow effective data sharing and communication with allies, still in development.[25] Perhaps most notably, given the prospect of grey zone challenges, consideration of peacetime engagement and its requirements have rarely been evident in army thinking or doctrine. Accordingly, a shift in the mindsets of the army (and CAF) will be essential for ensuring effective military modernization to address grey zone threats.

In the meantime, responses in the grey zone will likely be determined on a case-by-case basis in terms of coordinating efforts in a specific order, designating leadership (determined by the nature of particular threats as defined by actor, domain, and method of execution), and creating a framework outlining processes, procedures, and concepts. More work will be needed to address appropriate responses for cases not warranting a military response, including the action and which organization is best suited to respond. For example, is the Communications Security Establishment (CSE) better suited for offensive cyber activities than the CAF? Or should the CAF cyber command engage in active defences in the cyber domain?[26] It is essential to improve efforts to operationalize effectively the comprehensive approach to forge a truly integrated and collaborative means of addressing the security challenges that arise.

In addition, the multidimensional character of grey zone activities will require responses beyond the scope of the CA and the CAF and involve the highest levels of government, such as the Privy Council Office (PCO), the Prime Minister's Office (PMO), and the prime minister.[27] Canadian leadership must demonstrate credibility and resolve through an assertive posture. Consideration of the establishment of enforceable red lines, backed by current and developing Canadian strengths, such as AI, sensing, and connectivity, may be essential. Preparations through gaming and scenario development ("red teaming") will also be needed to enhance capability development through experience. This may lead to the adoption of CA actions and responses in the grey zone—innovative Canadian approaches to address "below the threshold activities" that have not been seen before (i.e., offensive actions in the cyber domain, in the electromagnetic spectrum, and psychological operations). An emphasis on effective signalling and messaging in these domains will also be a requirement, as perception management is key to deterrence in the grey zone, communicating red lines and the consequences of crossing them. At the tactical and operational levels, this involves deterring by detection and denial, and at the political-strategic level, deterrence by the threat of punishment (against some valued economic or highly strategic target).

The CA and CAF doctrine may need to consider adopting a "proactive deterrence" approach to manage the ambiguity of grey zone activity.[28] This involves taking initiative to anticipate and shape the strategic environment to establish advantage over the adversary. Such initiatives may include taking a page out of the adversary's grey zone playbook and creating ambiguity from the side of Canada and its allies to keep the adversary off balance and compelling them to reconsider taking certain actions, thereby enhancing deterrence.[29] In addition, the doctrine will need to reflect proportional responses for kinetic and non-kinetic effects in multiple domains and outline core competencies that need to be evolved and adapted for the grey zone.

In line with coordination between the military and other partners, a doctrine embracing proactive deterrence to address actors and activities that overlap the defence and security realms would be created. This must be based on enhanced intelligence collection, analytics, and information sharing (breaking down silos and filling gaps). This would move decision making and counter effects further left (i.e., before the threat emerges) so that the CA, the CAF, and Other

Government Departments (OGDs) are not reacting but anticipating and preventing threats before—or in the earliest stages of—being launched, allowing our forces to create a favourable operating environment.

Close Engagement and concepts for the "Army of Tomorrow" have already shifted thinking about how the CA would create effects in the multi-domain battlespace, including the grey zone. More needs to be done to move toward achieving capability, especially soldier training and education in areas not previously emphasized (e.g., history, politics, culture, and languages) to better assist with the development of responses to the grey zone strategies and tactics of potential adversaries; understanding "non-contact" warfare requiring enhanced Intelligence Surveillance Reconnaissance (ISR); and the application of operational tools, such as vignettes, for grey zone confrontation that consider questions at each stage of tactical activity through environmental scanning, operational frameworks, and legal and ethical considerations.[30] This process requires rethinking C2 and planning, capabilities, exercises, and enablers to facilitate a doctrinal shift to modernize the military for current and emerging grey zone threats.[31]

Conclusion

The CA and the CAF possess some of the capabilities to counter adversary activity in the grey zone, but more effort in developing a clear doctrine or approach to the grey zone is required. Modernizing the CA for the grey zone is impacted by budgetary constraints, gaps in available expertise in certain subject and technical areas, and revising priorities of the political leadership. In addition, many of the responses to the multidimensional nature of grey zone activities remain outside the CA and CAF's remit, requiring measures through OGDs and officials reaching the highest levels of Canadian leadership, as well as to the Five Eyes and other multinational partners. Thus, developing effective capability to respond to the grey zone is a government- and society-wide challenge.

Still, the need for CA and joint CAF initiatives to develop effective responses must not be ignored. This requires a shift in the CA's thinking and doctrine to deal with peacetime engagement, especially given the grey zone's characteristic blurring of peace and war. It also requires enhanced intelligence and sensing capabilities to allow for improved environmental scanning with the foresight to anticipate threats, tailor responses as quickly as possible, and move decisions and actions further left to shape the operating environment for greater advantage. The CA needs to increase its technical knowledge and develop competencies in key disruptive technologies to succeed in this endeavour. It must outpace the adversary to detect, deter, disrupt, and defeat hostile activities in the physical, space, cyber, and cognitive domains.

Beyond this, the CA must continue to pursue and actively promote the comprehensive approach to grey zone challenges. *Advancing with Purpose: The Canadian Army Modernization Strategy* (CAMS) describes relationships as the key to success.[32] Through partnerships and alliances, especially ABCANZ, NATO, and NORAD, DND and CAF engage in training exercises to enhance joint interoperability across multiple systems to improve intelligence mission data, joint communications, fires, information operations, and sustainment.[33] The emphasis on coordination and interoperability among joint, multinational partners—involving OGDs, allies, NGOs, academia, and the public—is well suited for the adaptation and agility required to respond to the ambiguity of grey zone activities. In the absence of wider government involvement, the effectiveness of efforts to address such challenges is likely to be limited.

About the Authors

Peter Gizewski is an Adjunct Professor in the Department of Political Science and Economics, Royal Military College of Canada (RMCC). A recently retired Defence Scientist with Defence Research and Development Canada's Center for Operational Research and Analysis (DRDC-CORA), he served as Strategic Analyst to the Canadian Army Land Warfare Center (CALWC) for over 20 years. He was educated at the University of Toronto (Trinity College) and Columbia University (Political Science/International Relations where he was a MacArthur Fellow in Conflict, Peace and Security and a Department of National Defence Fellow in Military and Strategic Studies). He also served as a core contributor to the CALWC's Future Army Project—a multi-volume study exploring the capability requirements for Canada's Army—circa 2040.

Dr. **Nancy Teeple** is a Defence Scientist-Strategic Analyst with Defence R&D Canada's Centre of Operational Research (DRDC-CORA) at CALWC in Kingston, Ontario. She is a research associate and adjunct assistant professor at the Department of Political Science and Economics at the Royal Military of College of Canada, a research fellow at the North American and Arctic Security Defence Network, and a member of the Center for Arctic Security and Resilience at the University of Alaska, Fairbanks.

Endnotes

[1] Literature describing the nature and implications of the grey zone and grey zone activity is growing. For useful overviews, see Kathleen Hicks et al., *By Other Means: Part 1 - Campaigning in the Gray Zone* (New York: Rowman and Littlefield, 2019); Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf; and Frank Hoffman, "Examining Complex Forms of Conflict, Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4, (November 2018): 30-47, https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf?ver=2018-12-04-161237-307.

[2] Canadian Army Land Warfare Centre (CALWC), *Close Engagement: Land Power in an Age of Uncertainty: Evolving Adaptive Dispersed Operations, Canadian Land Operations Capstone Operating Concept* (Kingston, ON: Army Publishing Office, 2019), 6.

[3] Emphasis added to highlight that Close Engagement includes the non-lethal aspect. CALWC, Close Engagement, 19.

[4] Elizabeth K. Kiessling, "Gray Zone Tactics and the Principle of Non-Intervention: Can 'One of the Vaguest Branches of International Law' Solve the Gray Zone Problem?," Harvard National Security Journal 12, no. 1 (February 2021): 122, https://harvardnsj.org/2021/02/volume-12-issue-1/.

[5] Morris et al., *Gaining Competitive Advantage in the Gray Zone*, 8.

[6] Atlantic Council, "Today's wars are fought in the 'gray zone.' Here's everything you need to know about it," Atlantic Council, February 23, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/#:~:text=While%20the%20United%20States%20has,allies%20without%20risking%20conventional%20escalation.

[7] Dani Belo and David Carment, "Grey Zone Conflict: Implications for Conflict Management," Canadian Global Affairs Institute (CGAI), December 2019, https://www.cgai.ca/grey_zone_conflict_implications_for_conflict_management.

[8] Rear Admiral John W. Tammen, "NATO's Warfighting Capstone Concept: anticipating the changing character of war," NATO Review, July 9, 2021, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

[9] The authors acknowledge the debate in strategic and operational studies regarding the use of grey zone as a concept describing hostile activities that blur the boundaries between peace and war, involving competitive actions below armed conflict (more accurately described as part of the spectrum of activities within the competition continuum). See US Marine Corps, "Competition Continuum," Joint Doctrine Note 1-19, June 3, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf. Mark Galeotti, among other scholars, addresses the danger of using the term grey zone (among others like hybrid warfare, unrestricted warfare) in modern warfare because it is so all encompassing that it loses meaning in distinguishing between activities that constitute peace versus war. See Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven: Yale University Press, 2022), 9-21; Donal Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid Warfare – Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (Winter 2020): 1-37.

[10] Kiessling, "Gray Zone Tactics," 149.

[11] Kiessling, "Gray Zone Tactics," 149.

[12] Hicks et al., *By Other Means*, 7.

[13] Hicks et al., *By Other Means*, 9.

[14] Hicks et al., *By Other Means*, 10-11; Ashley Lane, "Iran's Islamist Proxies in the Middle East," Wilson Center, January 24, 2023, https://www.wilsoncenter.org/article/irans-islamist-proxies; Seth G. Jones, "War by Proxy: Iran's Growing Footprint in the Middle East," Center for Security and International Studies, March 11, 2019, https://www.csis.org/analysis/war-proxy-irans-growing-footprint-middle-east.

[15] Hicks et al., *By Other Means*, 10-11.

[16] *Strong, Secure, Engaged: Canada's Defence Policy* conflates grey zone with hybrid activities, stating: "Hybrid methods involve the coordinated application of diplomatic, informational, cyber, military and economic instruments to achieve strategic or operational objectives. They often rely on the deliberate spread of misinformation to sow confusion and discord in the international community, create ambiguity and maintain deniability. … By staying in the fog of the gray zone, states can influence events in their favour without triggering outright armed conflict." Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 53, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.

[17] For instance, China's interest in investing in dual-use ports or air bases in Iceland or Greenland as part of its Polar Silk Road initiative has the potential to serve commercial and military purposes in the future. It can also dictate terms and control domestically, influencing and interfering in local and national politics and security, using debt-trap coercion. The Polar Silk Road is the Arctic aspect of China's Belt and Road Initiative – a strategy intended to develop a global infrastructure. See Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations Backgrounder, January 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[18] The activities described in this table are drawn from Morris et al., *Gaining Competitive Advantage*, 8-12.

[19] CALWC, *Close Engagement*, 19.

[20] Chatzky and McBride, "China's Massive Belt and Road Initiative," 6, 18, 34. For a discussion on the whole-of-government approach, see, Elzabeth G. Troeder, *A Whole-of-Government Approach to Gray Zone Warfare* (US Army War College Press, 2019), https://press.armywarcollege.edu/monographs/937.

[21] Chatzky and McBride, "China's Massive Belt and Road Initiative," 33.

[22] Chatzky and McBride, "China's Massive Belt and Road Initiative," 23, 38-41.

[23] There is already evidence of movement towards implementation as articulated in *Advancing with Purpose: The Canadian Army Modernization Strategy* (CAMS), which outlines four distinct elements of a constantly evolving and adapting force to meet the "demands posed by the adversary and their operating context": orientation in the strategic context; affirmation of the CA's contribution; confirmation of principles and priorities; and implementation of actionable efforts to position the CA for the future. CAMS indicates that the CA is modernizing and integrating within a larger joint pan-domain effort, where "the advent of capabilities in space, cyberspace, artificial intelligence, quantum computing, and others is changing militaries and their conduct of warfare." The CA is thus evolving to use these technologies "to best adapt and optimize concepts, operational efficiency, and organizational digitalization" in addition to evolving with competition in "the cognitive, moral, and physical planes." Indeed, the CA "will increasingly operate across a variety of mission sets, once considered non-traditional, to achieve GC objectives." Chapter 4 of CAMS outlines implementation in terms of lines of effort to evolve the CA that applies to the grey zone: a posture for concurrency, the human dimension, one-army integration, priority modernization initiatives that highlight digital transformation and R&D, particularly disruptive technologies exploited in the grey zone (space, robotics and automated systems, cyber, and AI), and a pervasive information environment. See *Canadian Army, Advancing with Purpose: The Canadian Army Modernization Strategy*, 4th ed. (Ottawa: Department of National Defence, December 2020), 30-55, http://www.army-armee.forces.gc.ca/assets/ARMY_Internet/docs/en/national/2021-01-canadian-army-modernization-en.pdf.

[24] See Canadian Army, "Modernization Vital Ground: Digital Strategy: The Essential Digital Pivot to be Effective in the Pan-Domain Fight," DND – HQ Canadian Army (June 2022), 2, 15, 19, 20, https://www.canada.ca/content/dam/army-armee/migration/assets/army_internet/docs/en/digit-strag/Digital_Strategy.pdf.

[25] See "4.1.1.2 Data Governance Activities of ADM(DIA)" and "6.4.3.2 Responsibilities of the Data Governors" at "DND/CAF Data Governance Framework," Government of Canada, last modified July 28, 2022, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/data-governance.html.

[26] For instance, "active defence" involves countering activities during or after they occur, versus offensive measures which attempt to deny through proactive action(s) to prevent or intercept the action before fully executed (i.e., shifting action to the left proactively rather than reactively). In the cyber domain, it is easier to attack than to defend, and offensive measures may provide more effective deterrence against would-be attackers. However, this depends on being able to attribute and locate the source of the attack. This new capability and associated doctrine may fit the mandate of CSE rather than the CAF. Alternatively, the CAF might consider evolving to adopt new roles in new domains (e.g., CAF undertaking active defence, CSE undertaking an offensive role).

[27] In this regard, greater effort must be made to develop and coordinate means to counter the use of disinformation campaigns by grey zone challengers by the government as a whole. Such efforts should include the creation of a warning system enabled by artificial intelligence (to deny the exposure of fake news to western media), and it would include containment through the development of a capacity to build immunity to disinformation campaigns. Here efforts would aim at developing and promoting counter narratives to prevent the propagation of disinformation by Western media and educating the public to the responsible use of social media and digital technologies. The development of a greater capacity for planning responses to grey zone threats is also required. This requirement, which would involve cross-government participation and oversight by government leaders for detailed planning and the conduct of rapid, enduring, and coordinated counter grey zone operations, has already been identified in the US by the Department of State. Yet in Canada, there is as yet no cross-governmental entity responsible for planning for grey zone response in advance. Accordingly, greater efforts should be focused on its creation. Beyond this, the ability and the willingness to apply comprehensive and whole-of-government approaches to meet the challenges that may arise in the grey zone must be strengthened considerably. For a detailed discussion of each of these points, see Maj. Alan Petrin, *Operationalizing the Gray Zone: A Challenge for Canada*, JCSP 45, Canadian Forces College, (Ottawa: Department of National Defence, 2019), https://www.cfc.forces.gc.ca/259/290/308/305/petrin.pdf.

[28] Proactive deterrence is an emerging concept better suited to the grey zone than any other type of competition, confrontation, or conflict. Here, the activities of criminal and proxy actors, (e.g., transnational criminal organizations, terrorist entities) could be addressed through effective use of the comprehensive approach – with intelligence

facilitated through interagency coordination and other relevant government departments, including those of allies and partners, to monitor suspicious activity from the cyber to the physical domain. Close Engagement's strong call for army participation in a comprehensive approach and the emphasis placed on enhancing CA capabilities in areas such as persistent surveillance, early warning and detection, and in data processing and analytics, could make a valuable contribution by providing the intelligence required for fashioning appropriate responses to those grey zone activities that occur. For an in-depth discussion of proactive deterrence, see Keith Culver and Michael Giudice, Concepts As Tools for Proactive Deterrence in the Pandomain, IDEaS Contract, F20-02666, (unpublished report, July 26, 2021).

[29] Maj. Declan Ward, *Moving Upstream: The Canadian Armed Forces in the Grey Zone*, JCSP 47, Canadian Forces College (Ottawa: Department of National Defence, 2021), 9-10. Ward addresses the impact of ambiguity in the grey zone, describing David Kilkullen's "liminal warfare" in which ambiguity is intended to keep the enemy unstable and ensure plausible deniability.

[30] For Russia's approach to non-contact warfare, see Michael Kofman, "Russia's armed forces under Gerasimov, the man without a doctrine," Riddle, April 1, 2020, https://www.ridl.io/en/russia-s-armed-forces-under-gerasimov-the-man-without-a-doctrine/.

[31] Canadian Army, *Advancing with Purpose*.

[32] Canadian Army, *Advancing with Purpose*, 9, 10, 35, 44, 48.

[33] ABCANZ "is an international program that promotes interoperability and standardization among the armies of the United States, Britain, Canada, Australia and New Zealand." Defense Standardization Program, "International Standardization," On ABCANZ, see "International Standardization," US Department of Defense, Accessed 18 July, 2023, https://www.dsp.dla.mil/Programs/International-Standardization/. See also Canadian Army, *Advancing with Purpose*, 10-11. Our assessment added NORAD as an essential joint partner for the defence of North America.

Army Sustainment in the Grey Zone: Emergent Technologies as Double-Edged Sword Challenges and Opportunities

Yazan Qasrawi, Peter Gizewski, Abdeslem Boukhouta, Peter Dobias, and Michael A. Rostek

Sustainment capacity—the ability to provide personnel, logistics, and other support required to maintain and prolong operations or combat—represents an essential component of military operations and is often directly related to success or failure on the battlefield.[1] The increasing use of grey zone tactics by adversaries (e.g., cyber-attacks or even the use of social media to disrupt sustainment routes by causing localized riots), combined with technological advances, raises questions regarding future sustainment and its conduct. What does effective sustainment involve, and how can it be realized?

To be operationally effective and efficient in the Future Land Operating Environment (FLOE) characterized by a proliferation of non-state actors, threats, and activities, the Canadian Army (CA) will require a modernized, robust sustainment system that integrates into its design defences against grey zone activities. Notably, emerging technologies may hold the key to achieving a competitive advantage for the CA in countering grey zone threats, such as disinformation and cyber-attacks. This is especially vital in the case of combat service support (CSS).[2] However, while technological advances can improve sustainment activities for the CA, they can also introduce new challenges. Adversaries can use them for grey zone activities to create vulnerabilities for the military. As the last line of logistics support to front-line units, the army is generally most susceptible to delays and disruptions. Even relatively minor delays in the resupply of ammunition or medical aid can have significant consequences on the battlefield.

The main contributions of this article are twofold. First, it explores the extent to which recent developments in networked technologies pertaining to CA projects may be employed to facilitate more effective sustainment of army operations in the grey zone and help counter military and non-military threats. Second, it identifies several challenges in the grey zone that might be encountered when attempting to sustain army operations. It also discusses the governance of the Canadian Armed Forces (CAF) and the CA in the grey zone and the lack of a policy framework for overcoming the identified challenges.

The article begins with a brief description of the grey zone and its characteristics, followed by a descriptive introduction to the concept of army sustainment. It then identifies select networked technologies that enable a digitalized military and hold promise for addressing challenges pertinent to grey zone operations. The identified technologies are primarily those that are considered by the CA, CAF, and allied armed forces as imperatives to modernize and digitalize CSS and improve sustainment capabilities across the multi-domain environment.[3] The article then discusses the challenges of harnessing such technologies and offers recommendations for the CA and CAF related to sustainment in the grey zone.

The Grey Zone

Grey zone operations, campaigns, or tactics refer to the use of non-military means to fulfill a political goal.[4] The underlying idea is to employ "unrelated innocent/low attributable, mutually-supporting and synchronised statecraft techniques" that achieve the objectives without making the targeted actor feel threatened enough to trigger a military response.[5] As a study from the Atlantic Council notes, "adversaries are increasingly pursuing their national objectives in a little-understood arena: the so-called gray zone between peace and open conflict."[6] Grey zone operations can include deniable attacks, information attacks, disinformation, employing proxy forces, economic coercion, territorial encroachment, cyber operations, election interference, and attacks involving electromagnetic weapons.[7] The deniability tends to vary depending on the action.

Beyond this, such threats are often technologically enabled, data-dependent (i.e., involving the use and manipulation of information to achieve specific goals), and rely on stealth, irregular and indirect approaches, subterfuge, and ambiguity to succeed.[8] They can work to delay, disrupt, and degrade capability, including sustainment, thus seriously reducing military effectiveness. Accordingly, responses to grey zone threats must be primarily information driven to facilitate comprehensive awareness of the environment and the threats within it and to devise strategies and tactics—defensive and offensive—to overcome attacks.

Army Sustainment in the Grey Zone

The US Army defines sustainment as "the provision of logistics, financial management, personnel services, and health service support necessary to maintain operations until successful mission completion."[9] In the era of renewed great-power competition and the growing threat of potential high-intensity conflict, the issue of sustaining major combat operations is gaining increasing attention. According to reports from the Russia-Ukraine war of 2022, the Ukrainian Army is spending thousands of artillery rounds a day, and consuming 15 million litres of fuel and other types of supplies.[10] In this context, logistics become the key enabler of combat operations. In competition or the pre-crisis era, deterrence remains crucial. A credible ability to move and sustain combat forces is a key element of deterrence, especially in the face of hostile anti-access capabilities.[11]

Operations below the threshold of a full-blown armed conflict or war introduce new challenges. One is the scale. While major combat operations require significant logistics capacity, credible deterrence requires the ability to move and sustain forces without acquiring and moving supplies. In other words, the national economies and sustainment networks need to have the ability to rapidly increase the production and movement of supplies when a crisis develops or a conflict commences.[12] It is worth noting that multiple agencies work continuously to support the armed forces for deployment, distribution, and even maintenance of platforms and assets. They also focus on addressing gaps in the sustainment network because adversaries can exploit them. Second, logistics are already contested through cyber, space and other means. Often, logistics can be opposed through other methods, such as blockades using civilians.[13] This situation is compounded by the limited legal authority of multiple agencies and departments and the fact that civilian authorities are often in control, which means that the military cannot unilaterally counter the challenges posed by the adversary, requiring time and effort to coordinate with other agencies to produce an effective solution.[14]

A variety of emerging technologies are transforming civilian logistics chains. The focus of these technologies is tracking sustainability concerns (including the cost of fuels), managing labour, investing in automation and robotics, enhancing integration of software solutions, and increasing

transparency.[15] The challenges of grey zone sustainment make it a prime candidate for adopting technological solutions. For example, implementing digital technologies might help forecast demand, thus reducing sustainment capacity requirements, streamlining maintenance, and helping protect sustainment networks from cyber-attacks and other disruptions. Likewise, western militaries—including the CAF—are adopting new technologies to address the threats and challenges posed in the grey zone and improve their sustainment networks.[16]

Emergent Networked Technologies and Implications for Army Sustainment

This section identifies several emerging, and existing, networked technologies that can enable digitalization and offer possibilities for addressing the challenges that may be encountered when attempting to sustain army operations in the grey zone. Indeed, such technologies may be helpful in effectively sustaining the conduct of land operations and bolstering the robustness of CA sustainment practices in the face of adversarial grey zone threats and challenges. However, they are also prone to weaknesses and gaps that adversaries can exploit to weaken a military's sustainment capacity and capability.

Artificial Intelligence (AI)

Given the critical importance of knowledge in the grey zone, artificial intelligence (AI), analytics, and advanced computing offer vital tools for the conduct of grey zone operations. One commentator notes: "The key to gray zone advantage is awareness. And AI's ability to rapidly process massive volumes of data lends it perfectly to situational awareness."[17] The result of using AI in army sustainment is a potential increase in the CA's capacity to conduct sustainment and CSS operations in a more secure, effective, and timely manner.

Maintenance operations of army platforms are traditionally planned based on mileage or usage of equipment, regardless of its condition.[18] AI and machine learning (ML) algorithms are enablers of predictive maintenance or automated proactive Health and Usage Monitoring Systems (HUMS) that are used to analyze collected data and predict when equipment will likely fail or need maintenance.[19] It is expected that all future CA platform acquisitions will have such capabilities. HUMS rely on automatic monitoring of maintenance requirements and are supposed to increase safety.[20] Notably, AI can utilize huge volumes of heterogeneous data to identify patterns and correlations that would be difficult to find by humans or rule-based methods.[21] By drawing and fusing data from multiple sources, such as past contingency and operational plans, AI and ML algorithms can be used by the CA to create automated analytics capabilities to improve coordination in its logistics planning process before and during military operations. These technologies can be used to predict the needed resources, assets, and equipment for each type of operation (e.g., to produce Tables of Equipment TO&E). It can then prioritize the most urgent information for the operator and aid decision making while avoiding cognitive overload. Also, CA logisticians can rely on AI or ML capabilities to continuously monitor a mission's logistics-related activities, such as projections and forecasts, stock levels of spare parts, asset positions, and asset conditions in Canada and abroad. Notably, those AI and ML algorithms can be vulnerable to theft and grey zone activities. However, an adversary (state or non-state actor) may be able to spoof the system and ground the entire fleet. Given this background, the CAF should not neglect security issues and adversarial attacks when implementing HUMS capabilities on army platforms. Technologies such as Blockchains or Distributed Ledgers can be used to protect such technologies and AI or ML developments.

Furthermore, while AI can be vulnerable to cyber- and electromagnetic (EM) attacks, secure and judicious use of the technology can offer considerable benefits.[22] The integration of AI into military systems helps streamline the conduct of sustainment and CSS through improvements in areas such as inventory management, the exposure of weak links in supply chains, the prediction of demand spikes and breakdowns in equipment, and the identification of resupply patterns. It also supports effective sustainment in the grey zone in multiple ways. For instance, AI may offer an essential tool for shaping the environment in which sustainment and CSS operations occur by providing a capability for developing information campaigns and influence activities that make environments more conducive to the conduct of operations. It can also offer a means of countering efforts by adversaries aimed at delegitimizing or degrading planned or undertaken operations (e.g., capacity building, humanitarian intervention, and peace support operations).

Beyond this, AI may also provide an important means of protecting sustainment and CSS capabilities against other types of adversarial attacks. Algorithms aimed at detecting and defending against data poisoning (manipulating training datasets by injecting false data to control the behaviour of the model and deliver false results), deep fakes (images or recordings that have been altered to misrepresent someone as doing or saying something that was not actually done or said), and cyber-attacks are likely to offer ever more essential means of increasing the security of information, and thus trust and confidence, in military supply chains—in peace and war.[23]

Supply Chain Digitalization and Grey Zone Activities

The coronavirus pandemic underlined that supply chains lack robustness and resilience and can be easily targeted by grey zone activities.[24] These vulnerable supply chains often support critical infrastructure (e.g., transportation networks) and thus offer a tempting target for adversarial action in the grey zone. Indeed, one needs only consider the economic costs and political turmoil associated with grounding the Ever Given container ship in the Suez Canal in March 2021 to appreciate the impacts that disruption of supply chains can cause.[25]

The Canadian Army Modernization Strategy (CAMS) states that "the supply chain will continue to be a risk area," implying that future supply chains may not be fully resilient or robust.[26] Digitalization can reduce this risk by providing data and information visibility to all parties involved in the CA's sustainment activities, creating transparency and trust in the supply chain. Consequently, supply chain vulnerabilities to grey zone activities can be mitigated by allowing the tracking and verification of the supply chain paths and components in real time.

To be sure, increasing reliance on connected information systems implies that Information and Communication Technologies (ICT) could represent a critical source of risk to defence. Connectivity will create vulnerabilities that adversaries can exploit. Accordingly, robust ICT supply chains and cyber security will be essential for resilience. Nevertheless, it is possible that digitalization technologies, such as digital twin (DT), Blockchains, and the Internet of Things (IoT), can eventually reinforce military supply chain networks' resilience and robustness and mitigate the risks associated with adversarial grey zone action.

Digital Twin (DT)

One of the most advanced and challenging approaches to digitalization is the development of reliable digital replicas of physical systems or processes under the concept of DT.[27] DT technology enables the user to monitor and control equipment and systems remotely.[28] It is enabled by consolidating large volumes of different data types, such as those provided by IoT sensors, and

presenting them into a "common view" or common operating or operational picture, in military parlance.[29] DT technology can analyze, optimize, predict, and control physical processes in real time. Ultimately, it can execute simulation models to test and predict asset and process changes under different hypothetical scenarios.

A Canadian Security Intelligence Services (CSIS) publication notes that smart cities represent the next generation of critical infrastructure that will be attractive targets for different actors and criminals for espionage, sabotage, and disruption. It also mentions that equipment and supply chains represent some of the methods that can be used to compromise smart cities.[30] Given this context, DT can provide capabilities to monitor critical infrastructures within a city or a country.[31] It is proactive rather than reactive in detecting anomalies resulting from the actions of grey zone actors.[32] The technology can also be used to build scenarios to examine the impact of cyber-attacks and identify associated abnormalities, resulting in robust smart cities and ensuring real-life cyber protection.[33] Moreover, its real-time monitoring capacity can provide added security against potential aggressors, allowing for the identification of cyber- and EM attacks and decoys in the digital space.

Furthermore, DT can play a crucial role in enabling the CA's digital journey, which is critical to army modernization. From a supply chain perspective, a Digital Supply Chain Twin (DSCT) is worthy of attention as well. DSCT is a real-time replica of the physical or the real-world supply chain or its specific segments. It combines all the data and models and updates itself from multiple sources. This networked technology can be applied to maintenance and logistics decision support to enable asset visibility and monitor supply chain processes, assets, and autonomous systems in real time.[34] Developing a high-performance DSCT can help improve operations, service innovation, and accelerate the delivery and the lead time of key assets. It can also ensure end-to-end visibility, traceability, and business continuity by enhancing predictive and reactive decisions using historical and real-time data analysis.

Blockchain

Blockchain is a technical solution for implementing the concept of trusted electronic distributed ledgers. These are distributed information-sharing systems supported by a protocol framework to control the performance of different types of transactions by any party to any other party's ledger.[35] The benefits of Blockchain have positive implications for the CA. To expand, CA operations are frequently carried out abroad with deployed network infrastructure with an increased risk of cyber-attacks against it.[36] These attacks threaten to degrade such infrastructure in the FLOE, often unbeknown to the operators.[37] Blockchains and electronic ledgers can empower ground-breaking innovations by protecting army network infrastructure from vulnerabilities, streamlining business processes, and reducing operating costs for CA logistics and sustainment.

Studies indicate that integrating Blockchain within logistic processes can improve the robustness and security of critical supply chains. Blockchain can enable the CA supply chain operations to be more efficient and transparent by securing the information exchange and business transactions between the different partners and stakeholders. This is done through a real-time secure information system that is accessible to the partners involved in a supply chain's transactions. The logistics component of the CAF Common Operating Picture project presents an opportunity to take advantage of this technology to secure the integrity of the data and information exchange and enable the implementation of the CA digitalization strategy.[38] Given its architecture, Blockchain offers a means of reducing inter-party mistrust while maintaining privacy and data confidentiality—conditions which may be especially beneficial for conducting coalition

operations.[39] Beyond this, the distributed structure of a Blockchain database minimizes the risk of cyber-attacks. It can also be used jointly with an Intrusion Detection System on cloud and IoT networks to protect the supply chain from cyber-attacks and safeguard private data.

The Internet of Things (IoT)

The IoT has already had a profound impact on the world. According to Statista reports, as of April 2023, approximately 64.6 per cent of the global population are internet users, with more than 60 per cent utilizing mobile phones to access it.[40] The rapid growth of IoT technology, then, has linked billions of objects. Its importance and utility for military sustainment is no exception. As one study notes, "The Internet-of-Things is a network of physical objects that are digitally connected to sense, monitor and interact within a Logistics Unit or institution and between this unit and its supply chain enabling agility, visibility, tracking and information sharing to facilitate timely planning, control and coordination of the supply chain processes."[41]

A digital data acquisition system is generally associated with the IoT network. This system can monitor, capture, control, or store information about the supply chain. Such capacity can also guard against cyber- and EM attacks, thus creating resiliency and robustness through redundancies in connectivity (i.e., if one part is attacked, information can be rerouted).

With the emergence of IoT on the battlefield, one of the challenges is securing the systems.[42] This is primarily because a full implementation of the IoT will have every electronic device connected to the network and will involve exchanging data. This considerably increases the number of entry points for cyber-attacks and could lead to added cyber vulnerabilities. Insider threats, user error, the use of jamming devices, electronic eavesdropping, or cyber malware are other serious risks to the network.[43]

The integrity of IoT data will be crucial, given its use in the decision loop. A major potential danger of the IoT is the risk of either an adversarial attack or a system failure that compromises the entire network. An IoT network compromised in this way can cause severe and irreparable damage through corrupted software, disinformation, and leaked intelligence. IoT devices, like everything connected to the internet, can be hacked and compromised or rendered useless. Even one vulnerable device can compromise the entire network.[44] These security risks are of particular concern in vehicle safety, healthcare, and supply chains. Hackers can potentially take over and steer vehicles.[45] Health and safety devices—such as drug-infusion pumps, heart monitors, and defibrillators—can be interfered with and controlled remotely.[46] The IoT device components manufactured and assembled worldwide for the military supply chain can be compromised as well.[47]

Battlefields are adversarial environments in which adversaries are expected to adapt and evolve their strategies for infiltrating the IoT. The IoT network must be continuously improved, preferably autonomously, to detect penetration through all available defensive mechanisms. Continuous improvement to keep the network secure and use counterintelligence measures will need a large-scale effort that may require the disposal of compromised devices and the use of honey-nets—a network set up as a decoy to catch attackers' attention and deceive them into thinking that they have gained access to a real system—that mislead enemy eavesdroppers.[48] Keeping the risks at a tolerable level will remain a continuous battle.

Challenges of Harnessing Technology in the Grey Zone

The potential of technologies to contribute to the effectiveness of sustainment and CSS in the grey zone is considerable. They can work to shape the environment to facilitate sustainment and CSS when it matters. Such systems can provide significant means for detecting threats and protecting systems from attack, as well as helping to ensure that sustainment and CSS are increasingly efficient and effective. There is a pressing need to continue to build an ecosystem to ensure the swift and effective development and integration of relevant technologies. Such an ecosystem will require adequate funds, relevant hardware, skilled personnel, and the development and hardening of networks, all of which would ensure interoperability with allies and partners through proper protocols, tactics, techniques, and procedures, as well as work to maintain trust and confidence in the deployed technologies.

At the same time, the CAF and the CA must recognize and address the fact that the same technologies that facilitate effective sustainment in the grey zone can lead to negative consequences. Grey zone threats pose a growing concern to effective sustainment and CSS. Adversarial grey zone activities can readily exploit the vulnerabilities in the supply chain, including those associated with critical infrastructure and its ICT system. That noted, emerging technologies such as AI, IoT, DT, and Blockchain offer considerable promise for reinforcing military supply chain network resilience and robustness and protecting it against challenges posed in the grey zone. Some of these technologies are a double-edged sword as adversaries and non-state actors can also use them for grey zone activities. In short, while representing potentially significant enablers in the right hands, they can be used for nefarious purposes when employed by adversaries (e.g., through cyber-attacks, the generation and spread of misinformation and disinformation, and data poisoning).

Given these possibilities, there is a need to rethink the role of the CA and CAF more broadly in the grey zone. A policy framework for approaches to grey zone challenges is currently lacking. ICTs (such as those discussed here) do not make logistics "smart," which is required to address challenges in the grey zone. It is worth noting that in many cases, integration of these technologies into military systems remains in the early stages, and much remains to be done.[49] There is a need to develop the human and social capital (i.e., networks of relationships among people who work in sustainment and CSS that enable them to function more efficiently and effectively), as well as a requirement for a broader anticipatory policy to leverage growth and manage CSS ICT in ways that make army logistics truly smart.

A proper governance framework for the application of IT systems to CSS is needed to mitigate stove-piped approaches and reduce potential vulnerabilities. Providing such a framework must not be an afterthought. A poorly implemented initiative risks doing more harm than good. A comprehensive approach to ICT is required to increase success in moving toward this governance framework. It is imperative to forge collaborative and cooperative processes with actors that fall beyond the traditional definition of CSS stakeholders to ensure that the technologies work in a synergistic, effective, and timely fashion.

Accordingly, a defence supply chain resilience strategy, which would include data and critical infrastructure, must be developed to counter grey zone activities. This would require continual assessment of the potential impacts of grey zone challenges on the CAF supply network (including the ICT system) and the further development and integration of those technologies deemed most promising for addressing the threats that grey zone activities pose. Concurrently, it would be worthwhile to develop a framework to ensure that such integration is conducted to maximize emergent technologies' capacity (and potential synergies) to address the challenges effectively. Such

efforts are essential to improving supply chain resilience and CAF preparedness in the face of grey zone challenges.

About the Authors

Dr. **Yazan Qasrawi** is a Defence Scientist with the Defence Research and Development Canada Centre for Operational Research and Analysis (DRDC-CORA) embedded at the Canadian Army Land Warfare Centre (CALWC), Kingston. Dr. Qasrawi's area of expertise is military and army logistics with a particular interest in emerging and disruptive logistics technologies and the application of modelling and simulation to military and army sustainment and logistics.

Peter Gizewski is an Adjunct Professor in the Department of Political Science and Economics, Royal Military College of Canada (RMCC). A retired Senior Defence Scientist with DRDC-CORA, he served as Strategic Analyst at the CALWC for over 20 years. He was educated at the University of Toronto (Trinity College) and Columbia University (Political Science/International Relations), where he was a MacArthur Fellow in Conflict, Peace and Security and a Department of National Defence Fellow in Military and Strategic Studies. He also served as a core contributor to the CALWC's Future Army Project—a multi-volume study exploring the capability requirements for Canada's Army—circa 2040.

Dr. **Abdeslem Boukhtouta** is a Senior Defence Scientist with DRDC-CORA. His expertise is in the domain of logistics and sustainment. He has conducted research on the optimization of logistics chains, sustainment and logistics resiliency and sustainability, and logistics modelling and simulations. Currently, he leads the Canadian Army Operational Research Team.

Dr. **Peter Dobias** is a Senior Defence Scientist with DRDC-CORA. He worked on analysis of complex and adaptive systems, including through wargaming and agent-based modelling; later, he led the analytical support to the Afghanistan mission assessment, including in-theatre support, followed by a three-year tenure as a Quantitative Analysis Team Lead at the Afghanistan Pakistan Center of the US Central Command in Tampa, Florida. Since 2019, he has been a Section Head for Land and Operational Command Operational Research, and continues pursuing research interests in complexity, hybrid warfare, wargaming, artificial intelligence, and data analytics.

Dr. **Michael A. Rostek**, CD, APF, is a veteran of the Canadian Armed Forces. He retired from the Regular Force in 2011 and served as a Reservist until 2022. He obtained his doctorate (War Studies) from the Royal Military College of Canada and holds two master's degrees—a Master of Management in Defence Studies from the University of Canberra, Australia, and a Master of Arts (Defence Management and Policy) from the Royal Military College of Canada. He has held several academic and research positions, primarily in the defence, security, and politics disciplines. He is currently employed as a Defence Scientist with DRDC-Toronto Research Centre as a member of the Intelligence, Influence and Collaboration section.

Endnotes

[1] US DoD/Transportation Command Defense Transportation Regulation, "Sustainment activities," III-304-1 June 2016, *United States Transportation Command*, https://www.ustranscom.mil/dtr/part-iii/dtr_part_iii_304.pdf; David Wilson, "Army Sustainment Capabilities Instrumental to the Joint Force in the Indo-Pacific Region," *Joint Force Quarterly* 108, no.

1, (2023): 67-74, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-108/Article/Article/3264632/army-sustainment-capabilities-instrumental-to-the-joint-force-in-the-indo-pacif/.

[2] Alan Estevez et al, "The Changing Character of Supply: Rethinking Logistics in an era of Systems Warfare," Modern War Institute, September 6, 2021, https://mwi.usma.edu/the-changing-character-of-supply-rethinking-logistics-in-an-era-of-systems-warfare/.

[3] Jordan Miller, Yazan Qasrawi, and Abdeslem Boukhtouta, *Technology Scanning for Combat Service Support (CSS) Modernization: An Investigation Study for the Canadian Army* (Ottawa, Canada: Defence R&D Canada, 2018).

[4] Anthony Robertson, "What is Grey Zone confrontation and why is it important?" The Cove, July 18, 2022, https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important.

[5] Anthony Robertson, "What is Grey Zone confrontation and why is it important?"

[6] "Today's wars are fought in the 'gray zone.' Here's everything you need to know about it," Atlantic Council, February 23, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/.

[7] For discussion on the various types of grey zone operations/activities, see "Competing in the Gray Zone: Countering Competition in the Space between War and Peace," *Center for Strategic & International* Studies, December 7, 2018, https://www.csis.org/analysis/competing-gray-zone-countering-competition-space-between-war-and-peace; Stacie L Pettyjohn and Becca Wasser, *Competing in the Gray Zone Russian Tactics and Western Responses* (Santa Monica, CA: RAND Corporation, 2019), https://apps.dtic.mil/sti/pdfs/AD1088607.pdf.

[8] Carvent L. Webb II, "Understanding the Gray Zone: How Federal Law Enforcement Agencies Can Support SOF Operations Related to Counterterrorism Strategy," *American Intelligence Journal* 37, no. 1 (2020): 183–89, https://www.jstor.org/stable/27087697. On information operations in the grey zone, see, Ashley Mattheis et al., "Blind Sided: A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone," Irregular Warfare Center, March 14, 2023, https://irregularwarfarecenter.org/publications/research-reports/blind-sided-a-reconceptualization-of-the-role-of-emerging-technologies-in-shaping-information-operations-in-the-gray-zone/.

[9] U.S. Department of the Army, *Army Doctrine Publication 4-0 Sustainment* (Washington, DC: Headquarters, Department of the Army, 2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18450_ADP%204-0%20FINAL%20WEB.pdf.

[10] Camille Grand, *A question of strategic credibility: How Europeans can fix the ammunition problem in Ukraine*, European Council on Foreign Relations, April 2023, https://ecfr.eu/article/a-question-of-strategic-credibility-how-europeans-can-fix-the-ammunition-problem-in-ukraine/; Rosemary Griffin et al., "Ukraine war sees diesel prices rise as Russia's thirsty battle tanks guzzle fuel," S&P Global, May 2022, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/052322-ukraine-war-sees-diesel-prices-rise-as-russias-thirsty-battle-tanks-guzzle-fuel.

[11] Michael Roi, *Hybrid Warfare, Deterrence in the Baltics and Escalation Dominance*, DRDC-RDDC-2018-L121, May 2018.

[12] Harry F. Ennis, *Peacetime Industrial Preparedness for Wartime Ammunition Production* (Washington D.C.: National Defense University, 1980), https://apps.dtic.mil/sti/tr/pdf/ADA089978.pdf.

[13] Greg Lewis, "Highway to the Gray Zone," *Proceedings* 148, no. 9 (September 2022), https://www.usni.org/magazines/proceedings/2022/september/highway-gray-zone; Paul P. Murphy and Josh Pennington, "Ukrainians try to block Russian tanks with their bodies and bicycles," *CNN*, February 26, 2022, https://www.cnn.com/europe/live-news/ukraine-russia-news-02-26-22/h_aabb90712d1378fd1446f84d86815fb5.

[14] Ashley J. Roach, "Rules of Engagement," *Naval War College Review* 36, no. 1 (1983): 46–55, http://www.jstor.org/stable/44642842.

[15] Rajesh Kumar, "Emerging Trends in Technology for Logistics in 2023," Supply and Demand Chain Executive, March 2023, accessed August 3, 2023, https://www.sdcexec.com/sourcing-procurement/erp/article/22766836/ramco-emerging-trends-in-technology-for-logistics-in-2023.

[16] "Canadian Armed Forces – Operational Sustainment Modernization Strategy," Government of Canada, last accessed August 7, 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-operational-sustainment-modernization-strategy.html.

[17] *Confidence in Chaos: How to use emerging technologies to combat grey zone threats* (Farnborough, UK: QinetiQ, September 2020), 52, https://www.qinetiq.com/en/insights/grey-zone-warfare.QinetiQ.

[18] U.S. Department of the Army, *Army Technical Publications Maintenance Operations* (Washington, DC: Headquarters, Department of the Army, July 2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN19571_ATP%204-33%20C1%20FINAL%20WEB.pdf.

[19] K. F. Fraser, *An Overview of Health and Usage Monitoring Systems (HUMS) for Military Helicopters* (Victoria, Australia: Department of Defence, 1994), https://apps.dtic.mil/sti/pdfs/ADA289903.pdf.

[20] "Health Usage Management Systems (HUMS): Enhance flight safety, efficiency and maintenance," Collins Aerospace, last accessed August 7, 2023, https://www.collinsaerospace.com/what-we-do/industries/helicopters/rotary-wing/health-usage-management-systems.

[21] "Artificial Intelligence in Maintenance," Nanoprecise, last accessed August 7, 2023, https://nanoprecise.io/artificial-intelligence-in-maintenance/.

[22] Marcus Comiter, *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It* (Cambridge, MA: Belfer Center for Science and International Affairs, August 2019), https://www.belfercenter.org/publication/AttackingAI; Kai Fang et al., "Detection of weak electromagnetic interference attacks based on fingerprint in IIoT systems," *Future Generation Computer Systems* 126 (January 2022): 295-304, https://doi.org/10.1016/j.future.2021.08.020.

[23] At the same time, ongoing advances in AI will likely generate tension between offensive and defensive applications of AI technology and ever more intense competition among rivals to gain decisive military advantage from AI-enabled systems. Accordingly, advantages offered by the application of AI, both in the grey zone and beyond it, may well be limited or even fleeting, given the passage of time. For discussion on deep fakes and data poisoning, see Xiaoyu Cao and Neil Zhenqiang Gong, "Understanding the Security of Deepfake Detection," in *Digital Forensics and Cyber Crime: 12th EAI International Conference, ICDF2C 2021, Virtual Event, Singapore, December 6-9, 2021 Proceedings*, eds. Pavel Gladyshev et al. (Cham, Switzerland: Springer, 2022), 360-378; Sara Newman, "Detecting targeted data poisoning attacks on deep neural networks" (PhD diss,. University of Missouri-Columbia, May 2022), https://mospace.umsystem.edu/xmlui/handle/10355/94192.

[24] See Andrew Dowse and John Blackburn, "Improving Supply Chain Resilience through Preparedness," *Security Challenges* 16, no. 4, (2020): 82-98. https://www.jstor.org/stable/26976259.

[25] The incident placed considerable pressure on global supply chains and impacted supply distribution around the world. The Suez Canal accounts for approximately 30 per cent of the world's daily shipping container freight. See "The Importance of the Suez Canal to Global Trade," New Zealand Foreign Affairs and Trade, last updated April 18, 2021, https://www.mfat.govt.nz/en/trade/mfat-market-reports/the-importance-of-the-suez-canal-to-global-trade-18-april-2021/#:~:text=The%20193km%20Suez%20canal%20was,worth%20of%20goods%20per%20annum.

[26] Canadian Army, *Advancing with Purpose: The Canadian Army Modernization Strategy*, 4th ed. (Ottawa: Department of National Defence, December 2020), 29, http://www.army-armee.forces.gc.ca/assets/ARMY_Internet/docs/en/national/2021-01-canadian-army-modernization-en.pdf.

[27] Behaviours and relationships can also be included here.

[28] Different concepts are associated with digital twins, such as Digital Shadow and Digital thread. However, digital twin is the term generally used when simulations are used to do predictions about the future of the system. For an introductory discussion, see Derek Fanton, "Digital Twins: Examples and Use Cases," Onlogic blog, July 21, 2022, https://www.onlogic.com/company/io-hub/digital-twins-examples-and-use-cases/.

[29] Josh Triantafilou, "The role of digital twins in smart cities," Esri Canada, August 27, 2021, https://resources.esri.ca/news-and-updates/the-role-digital-twins-in-smart-cities.
According to the U.S. Department of Defense Dictionary of Military and Associated Terms, common operating (or operational) picture refers to "automation services that support the development of the common reusable software modules that enable interoperability across multiple combat support applications." See U.S. Department of Defense, *Joint Publication 1-02* (Washington, DC: Headquarters, Department of Defense, 2001 [amended through 2008]), https://web.archive.org/web/20081123014953/http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[30] "Smart Cities and National Security," Government of Canada, last modified February 16, 2022, https://www.canada.ca/en/security-intelligence-service/corporate/publications/smart-cities-national-security/smart-cities-national-security.html.

[31] DT is considered a critical tool for realizing smart cities. Smart city can refer to environments where digital technologies are used to enhance the quality and efficiency of the different services provided by a municipality. See smart city definitions provided in "Smart Cities and National Security," Government of Canada, last modified February 16, 2022, https://www.canada.ca/en/security-intelligence-service/corporate/publications/smart-cities-national-security/smart-cities-national-security.html.

[32] Pablo Calvo-Bascones et al., "A collaborative network of digital twins for anomaly detection applications of complex systems. Snitch Digital Twin concept," *Computers in Industry* 144 (January 2023), https://doi.org/10.1016/j.compind.2022.103767.

[33] Richard J. Somers et al., "Digital-twin-based testing for cyber–physical systems: A systematic literature review," *Information and Software Technology* 156 (April 2023), https://doi.org/10.1016/j.infsof.2022.107145.

[34] Mukesh Dialani, "Digital Twins — Transforming Supply Chains and Operations," Spotlight, March 2022, https://www.ibm.com/downloads/cas/LVJKXXNA.

[35] With the advent of this trusted distributed ledger, several supply chains can now use smart contracts, which are computer codes that run on the top of Blockchain technology.

[36] To learn more about the vulnerabilities of deployed network, see, Fabio Mulazzani and Salvatore Alessandro Sarcià, "Cyber Security on Military Deployed Networks," (paper presented at the 3rd International Conference on Cyber Conflict Tallinn, Estonia, 2011): 13-27, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ccdcoe.org/uploads/2018/10/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf.

[37] Fabio Mulazzani and Salvatore Alessandro Sarcià, "Cyber Security on Military Deployed Networks."

[38] Department of National Defence (DND), "DRAFT - Strategic J4 – Recognized Logistics Picture (RLP) Strategy and Implementation Plan," (Ottawa: DND Canada, September 2020) cited in Dwayne E. Demers, "Improving Logistics Operational Effectiveness and Efficiency Through Modernization for a Future Operating Environment" (Canadian Forces College, 2021), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cfc.forces.gc.ca/259/290/23/286/Demers.pdf.

[39] For useful discussions of Blockchain and its applications in defence, see James Gatto and Townsend Bourne, "Blockchain Tech Has Numerous Applications for Defense," *National Defence Magazine*, December 11, 2019, https://www.nationaldefensemagazine.org/articles/2019/12/11/blockchain-tech-has-numerous-applications-for-defense.

[40] Ani Petrosyan, "Number of internet and social media users worldwide as of April 2023," Statista, last accessed July 18, 2023, https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=As%20of%20April%202023%2C%20there,percent%20of%20the%20global%20population; "Mobile internet usage worldwide - Statistics & Facts," Statista, last accessed July 18, 2023, https://www.statista.com/topics/779/mobile-internet/#topicOverview.

[41] Michael J. Mic Martin, Stacey R. Kidd, and Christopher B. Landis, "5G Technology: Improved Capabilities Enable Joint Logistics for the Future Joint Force," U.S. Army, April 13, 2020, https://www.army.mil/article/234375/5g_technology_improved_capabilities_enable_joint_logistics_for_the_future_joint_force.

[42] SRI International, "SRI International Leading Security Research for U.S. Army Research Lab Initiative to Develop and Secure the Internet of Battlefield Things (IoBT)," *Cision PR Newswire*, February 21, 2018, https://www.prnewswire.com/news-releases/sri-international-leading-security-research-for-us-army-research-lab-initiative-to-develop-and-secure-the-internet-of-battlefield-things-iobt-300601689.html.

[43] Matej Tonin (Rapporteur), "The Internet of Things: Promises and Perils of a Disruptive Technology," *NATO Parliamentary Assembly Science and Technology Committee*, 081 STCTTS 17 E (August 28, 2017), https://www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis.

[44] See Arielle Pardes, "The WIRED Guide to the Internet of Things," *Wired*, September 11, 2020, https://www.wired.com/story/wired-guide-internet-of-things/; Matt Burgess, "What is the Internet of Things? Wired explains," *Wired*, February 16, 2018, https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

[45] Bruce Schneier and Tarah Wheeler, "Hacked drones and busted logistics are the cyber future of warfare," Brookings, June 4, 2021, https://www.brookings.edu/articles/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.

[46] Ashleigh Webber, "Hacking of "vulnerable" wearables and health devices could be fatal, warns report," *Personnel Today*, March 21, 2018, https://www.personneltoday.com/hr/health-technology-hacked-consequences/#:~:text=Health%20technology%20such%20as%20pacemakers,the%20Royal%20Academy%20of%20Engineering.

[47] Greg Hadley, "Hacking the Supply Chain," *Air and Space Forces Magazine*, December 3, 2021, https://www.airandspaceforces.com/article/hacking-the-supply-chain/.

[48] Javier Franco et al., "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials* 23 no. 4, (2021): 2351-2383, https://dblp.org/rec/journals/comsur/FrancoACU21.html. To read more on cyber counterintelligence, see, Petrus Duvenage and Sebastiaan von Solms, "The case for cyber counterintelligence," (paper presented at International Conference on Adaptive Science and Technology, Pretoria, South Africa, 2013): 1-8, 10.1109/ICASTech.2013.6707493.

[49] "Digital experiments: Under new digital strategy, more tech trials from the ground up," *Canadian Army Today*, July 24, 2023, https://canadianarmytoday.com/digital-experiments-under-new-digital-strategy-more-tech-trials-from-the-ground-up/.

Narrative as a Force Multiplier in the Information Battlefield

Suzanne Waldman

The need to "win the battle of narrative" has been a constant refrain in Canadian military circles.[1] For more than a decade, theorists and international policymakers have advocated for militaries to compete in this battle by leading their operations and strategies with deliberate, consistent, and well-communicated narratives.[2] Yet the process of standardizing a narrative-driven military communication process has been fraught, and many projects with such an aim have been launched and put to rest during this period, including in Canada.[3]

A major obstacle to military narrative communication is public disagreement about what types of communication are acceptable for governments and militaries, particularly where the line falls between acceptable information and unacceptable propaganda.[4] Another obstacle is a lack of institutional understanding of how to "narrate" significant events in ways that will engage key audiences, especially on social media, where the narrative battle is intense.

This article makes the case that narrative practice is a benign and necessary approach to governmental and military communication in the current age. It also argues that new means of institutional narration must incorporate five key factors: timeliness and consistency; dedicated practices; craft; awareness; and tools and policy.

Timeliness and Consistency

Over the past five years, Canada and other democracies have been on their back feet with respect to public communication about emerging events. Governments and militaries are, in theory, well placed to narrate meaningfully many types of unfolding events to the public, given all the experts they employ to understand and contextualize these events. Yet politicization of government communications incentivizes planned and bland communications over timely commentary.[5] For militaries, barriers to timely commentary on current events are even higher due to the culture of operational security as well as civil-military requirements that militaries must follow rather than set national narratives.[6]

The result: when defence-related events occur, the Canadian government's account of those events is quite likely to be preceded on social media by others' accounts, including those of Canada's adversaries, who can seize the lag to introduce narratives that will "anchor" global audience perceptions of those events at the point when they are most avidly engaged in them.[7] An example of adversaries exploiting a narrative gap can be observed early in the Russian invasion of Ukraine. A recent University of Calgary study has found that during the first month of the war, at least 25 per cent of the content being exchanged by Canadian accounts on Twitter (renamed as X) was pro-Russian narratives circulated by primarily Russian and American sources.[8] Subsequent research showed Canadians who prefer to obtain their news through social media were likely to have been influenced by at least some of these narratives.[9]

Importantly, during that same period, Canadian government ministers were advancing in press conferences a strong narrative about how the Russians were violating the territorial sovereignty of Ukrainians, as well as long-standing international norms.[10] Yet a scan of the Government of Canada's social media account activity in the first few weeks of the invasion shows

that it hewed almost entirely to pre-planned messaging. Suppose social media communicators instead had the mandate to support real-time narration in the online space. In that case, they might have speedily turned ministerial statements into digestible, sharable posts conveying a morally and factually authoritative perspective on the invasion, filling the narrative vacuum Russia partially occupied at a key point in the conflict.

Government practices of filling the information environment with true, current, regular, and engaging updates on events and issues can be classed as "cognitive defence."[11] These practices—along with building the national ability to recognize disinformation—are regarded as some of the most important elements of building national resilience against adversarial narrative campaigns.[12] With Canada's competitors developing increasingly sophisticated capabilities to spread disinformation in our media and social media environments—increasingly via artificial intelligence tools—cognitive defence should be regarded as an essential mandate for government communicators, including, and perhaps especially, defence communicators.[13]

Efforts by Canadian government departments to counter Russian disinformation about Ukraine have since made a promising shift in the right direction, as seen in the social media posts of Global Affairs Canada and Canadian Forces Intelligence Command from mid-2022 onward. These debunking posts represent a strong step toward government communicators engaging in narrative competition on social media. Yet insofar as debunking posts capture not only Russian disinformation, but also the facts that dispel the disinformation, they suggest that governments would benefit from putting out more real-time truthful information on defence-related events, as they break to "prebunk" disinformation and keep it from taking hold at the outset.[14]

Image 1: Social media post issued by the Global Affairs Canada.[15]
Source: Screenshot provided by the author.

Image 2: Social media post issued by the Canadian Forces Intelligence Command.[16]
Source: Screenshot provided by the author.

Over the past year, an especially strong performer on social media has been the UK Ministry of Defence (MoD), which has tweeted out declassified intelligence and maps on the Russian invasion of Ukraine virtually daily, elevating itself as a reliable source of timely and authoritative information.[17] The UK MoD not only provides updated authoritative information on events in the news, but it also regularly supplies wider context and analysis, shedding light on those events. This practice can be termed "strategic sensemaking" because it contextualizes those events within wider arcs and frames, and helps account for policy decisions related to them. As the post below shows, the UK MoD's updated informational maps are consistently accompanied by the department's strategic narrative that the Russian invasion of Ukraine was "illegal and unprovoked," therefore Ukraine deserves persistent support in repelling it.

Image 3: Social media post by the UK Ministry of Defence.[18]
Source: Screenshot provided by the author.

Narrative practices

As the UK MoD tweet above shows, narration involves more than just supplying isolated pieces of information. While information concerns the "who," "where," "when," and "what" of events, narratives also make inferences about the "why" and "so what" by interpreting patterns such as causality and similarity between events.[19] Supplying these inferences is highly important, as without narratives to hold events together, our minds tend to either remain confused or use the narratives offered by others, some of which may be designed to distort our perspectives.[20] As the table below demonstrates, a narrative is advanced through a set of practices that contextualize events or situations by relating them to each other and the larger backdrops of the world.

Narrative Practices for Contextualizing Events and Situations
Interpretation – isolating important patterns
Iteration – demonstrating or exemplifying a narrative pattern repeatedly
Exemplification – highlighting instances—that is, stories—that reflect patterns
Association – comparing novel events or situations to more familiar ones

Table 1: Narrative Practices for Contextualizing Events and Situations.
Source: Author

The importance of narrative practices can be seen in coronavirus communication, where institutional delivery of information and data has been noted to fall flat among many citizens, and

narrative has been assessed as a more effective vehicle.[21] Among the narrative practices listed above, Japan's Public Health Agency's memorable *interpretation* of the "Three Cs" of high-risk situations—Closed Spaces, Crowded Places, and Close-Contact Settings—empowered its citizens and stood the test of time.[22] A successful use of *iteration* was Taiwan's Central Epidemic Command's Centre's daily use of Zongchai—the media manager's Shiba Inu—as a mascot in coronavirus-related messages, with the dog attaining popularity both as a meme and a national hero.[23]

Image 4: Social media post by Taiwan's Central Epidemic Command's Centre.[24]
Source: Screenshot provided by the author.

Closer to home, memorable Canadian coronavirus communications *exemplified* stories of individuals who contracted the virus. The case of Sophie Grégoire Trudeau, the prime minister's wife (separated in 2023), in 2020 saw Justin Trudeau cast as an early exemplifier of "the prescribed way to prevent further spread of the disease" via the press conferences that he conducted outside of his home.[25] Later in 2021, Canadian public health experts advanced a relatable *association* between multi-layered protection against coronavirus and a hockey team that fields a forward line, a defence pairing and a goalie to keep the opposing team from scoring against them.[26]

These examples of coronavirus-related communication demonstrate how government communicators in the era of social media must not merely provide information but make it narratively digestible, poignant, and relatable. They also indicate how our human need for patterns calls on government and military communication narration to be maintained consistently (ideally, daily). Taiwan's daily public health communications featured the Shiba Inu as a COVID mascot. In contrast, the Canadian association between the coronavirus and hockey was made only a few times and shows little sign of having penetrated Canadian consciousness. Only when information is contextualized through consistent practices of narration does it have a good chance of being noticed, shared, and applied by individuals making sense of a complex world.

Narrative Craft

Were a decision made to place narration at the centre of public communication, the next question would be "how"? The most important thing to understand about narratives is that, even though we use them to make sense of new situations, they virtually always match pre-existing frames with which we are already familiar.[27] Helpfully, Canadian literary critic Northrop Frye described four well-known narrative frames with deep roots in Western culture that can play a helpful role in guiding the creation of narratives: *comedy*, *romance*, *tragedy*, and *irony*. In a comedy, there is minor turbulence, but the status quo is under control and sustainable. In a romance, the ground is shifting radically—although whether for better or worse will depend on the courage and valour of participants. In a tragedy, all hope in current structures is lost, and grieving and a hard shift are required. In irony, change is overdue, and the only recourse is dark, absurd humour. These four traditional narrative frames structure the great stories of entertainment, politics, and even religion through typical arrangements of plot, characterization, imagery, emotion, and values.[28] Drawing appropriately on these narrative moulds can help defence communicators stay true to the government perspective while connecting with a wide range of audiences, given their familiarity with age-old—and yet still highly current—narrative traditions.

Narrative Awareness

On participative social media, whenever anyone selects words and images to make a point, a story is likely to be told—whether deliberately by the original source, or through the follow-on storytelling of others. Narrative awareness is having the foresight of the story likely to be told by or about an incident or communication before it happens.

A tweet from a former Canadian Armed Forces (CAF) chief of the defence staff in 2021 provides an example of how narrative awareness could have averted a serious communication misstep. The tweet (see the image below) featured a romantic message about building diversity and inclusion that fundamentally involves combatting the status quo. But the image accompanying it was of seven white men in a boardroom, reinforcing a comic narrative of institutional leaders maintaining the status quo and highlighting a "say-do gap" in the organization. When observers noticed the mismatched narrative frames in the text and image, the CAF became the butt of ironic jokes. This case demonstrates how narrative is bound to happen whether we are intentional about it or not—so it is best to be intentional about it.

Image 5: Social media post by former Canadian Armed Forces chief of the defence staff.[29]
Source: Screenshot provided by the author.

In contrast, a tweet about diversity and inclusion posted by the Canadian Forces Liaison in Washington's @CAFinUS account in 2020 demonstrated how to deploy a narrative frame with intentionality. This tweet featured a picture of a male CAF soldier returning from deployment kissing his boyfriend, appended with the hashtag #proudboys—a response to a challenge from influencer George Takei to "troll" the right-wing extremist group Proud Boys.[30] This tweet presented the CAF as a vanguard romantic organization that celebrated its gay troops and had an online cachet. The massively positive response to this tweet demonstrates how knowingly working with narrative frames can help an institutional account gain the positive moral high ground and attention in a crowded information environment.

Image 6: Social media post by the Canadian Forces Liaison in Washington.[31]
Source: Screenshot provided by the author.

Narrative Tools and Policies

While narrative practice can be as much of an art as a science, building a savvier approach to social media communication benefits strongly from data, especially in expeditionary contexts. Automated tools could be used to provide situational awareness of narratives on social media, supporting the quick debunking of potentially dangerous disinformation and the filling of informational gaps while maintaining the privacy of Canadian citizens in keeping with the National Defence policy.[32]

Updated communication policies may also be required to support narrative practices. The communication policies of the Treasury Board of Canada call for departments to release only "objective" information to maintain public trust.[33] Yet recent research shows that public trust is also founded on the belief that governments are benevolent, which suggests that evoking values of care and emotions of concern may be just as important.[34] How to evoke relatability as well as reliability through appropriate advocacy of values and expressions of emotions in institutional communications is a question being reconsidered in the social media era.[35]

The most important requirement for engaging in the online battle of narratives is for communicators to be empowered to operate closer to the speed of social media. In military parlance, this objective would be facilitated by mission command processes that do not require the highest levels of government approval for every message released. Ideally, when new issues arise, communication managers would be permitted to create narrative guidance quickly, and communications teams would be entrusted to deliver narratively aligned social media content that responds to relevant events and the social media moment.

Conclusion

One of the aims of this article is to demonstrate how militaries can be competitive actors in digital and social media, playing to win the narrative battles in the information environment. Undoubtedly, competing strategically and tactically on the level of narrative will require new communication-related attitudes, processes, tools, and policies. The following are some general tips:

- Implement strategic sense-making mandates and practices that empower communicators to narrate issues in terms of their implications for national interests and values in ways that are engaging as well as informative; and
- create policies that delegate down social media communication responsibilities to departmental and unit teams, so government communicators can swiftly explain and contextualize events as they arise for audiences on social media, and quickly address counter-narratives developing through disinformation.

In the era of social media, no one is exempt from telling stories—or from anticipating the stories based on their own and others' actions. It is, therefore, crucial for militaries and governments to be aware of how they and their interests are implicated in the narratives circulating on social media, and to fill narrative vacuums that will otherwise be exploited by Canada's adversaries.

About the Author

Dr. **Suzanne Waldman** is a Defence Scientist with Defence Research and Development, working on topics associated with communication and countering disinformation. She has a Ph.D. in English Literature from Dalhousie University and a Ph.D. in Communication Studies from Carleton University.

Endnotes

[1] Jack Burnham, "Losing the Narrative? The Struggle of The Canadian Armed Forces to Shape Its Image," NATO Association of Canada, July 5, 2021, https://natoassociation.ca/losing-the-narrative-the-struggle-of-the-canadian-armed-forces-to-shape-its-image/.

[2] Mark A. Finlayson & Steven R. Corman, "The Military Interest in Narrative," *Sprache und Datenverarbeitung* 1-2 (2013): 173-191, https://users.cs.fiu.edu/~markaf/doc/j2.finlayson.2013.sdv.37.173_archival.pdf.

[3] Brett Boudreau, "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," Canadian Global Affairs Institute (CGAI) May 2022, https://www.cgai.ca/the_rise_and_fall_of_military_strategic_communications_at_national_defence_2015_2021.

[4] Dave Scanlon, "Canadians should hear the plain truth from their armed forces says retired senior Public Affairs officer," *Ottawa Citizen*, July 15, 2021, https://ottawacitizen.com/news/national/defence-watch/canadians-should-hear-the-plain-truth-from-their-armed-forces.

[5] Brent Barnhart, "Social media and government: how to keep citizens engaged," Sprout Social, January 13, 2022, https://sproutsocial.com/insights/social-media-and-government/.

[6] Peter D. Feaver, "The Civil-Military Problematique: Huntington, Janowitz, and the Question of Civilian Control," Armed Forces & Society 23, no. 2 (1996): 149-178.

[7] Taha Yasseri and Jannie Reher, "Fooled by facts: quantifying anchoring bias through a large-scale experiment," *Journal of Computational Social Science* 5 (2022): 1001–1021.

[8] Jean-Christophe Boucher et al., "Disinformation and Russia-Ukrainian War on Canadian Social Media," SPP Briefing Paper, *The School of Public Policy Publications* 15, no. 1 (June 2022), https://www.policyschool.ca/wp-content/uploads/2022/06/Briefing.DisinfoRussiaUkrWar.pdf.

[9] Anatoliy Gruzd et al., "The Reach of Russian Propaganda & Disinformation in Canada: A Canada-Wide, Census-Balanced Survey," Social Media Lab, Toronto Metropolitan University (2022), https://doi.org/10.6084/m9.figshare.20277855.

[10] Justin Trudeau, "PM Trudeau announces more weapons for Ukraine in response to Russian invasion - February 28, 2022," filmed February 28, 2022, YouTube video, 42:16, https://www.youtube.com/watch?v=hz1eVFFLxqQ.

[11] Marcus Kolga, "The growing threat of Russian information operations against Japan: Marcus Kolga for Inside Policy," Macdonald-Laurier Institute, May 24, 2023, https://macdonaldlaurier.ca/the-growing-threat-of-russian-information-operations-against-japan-marcus-kolga-for-inside-policy/.

[12] "Mapping and Analysis of Efforts to Counter Information Pollution in Europe and Central Asia Region," United Nations Development Program, December 22, 2023, https://www.undp.org/eurasia/publications/information-pollution.

[13] Graphika, "Deepfake It Till You Make It," (February 2023), https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf.

[14] "NATO's approach to countering disinformation: a focus on COVID-19," North Atlantic Treaty Organization, last modified July 17 2020, https://www.nato.int/cps/en/natohq/177273.htm.

[15] Global Affairs Canada (@CanadaFP), Twitter (renamed as X), September 6, 2022, 11:04 a.m., "We're working with international partners to detect, correct and call out the Kremlin's state-sponsored disinformation about Ukraine. See more facts versus Russia's false claims:," Twitter (renamed as X), September 6, 2022, 11:04 a.m., https://t.co/5O4HgYgctu.

[16] Canadian Armed Force (@Canadian Forces), "We're working with international partners to detect, correct, and call out the Kremlin's state-sponsored disinformation about Ukraine. Read the latest information based on Canadian Forces Intelligence Command analysis," Twitter (renamed as X), September 1, 2022, 4:05 p.m., https://twitter.com/CanadianForces/status/1565430568380145664.

[17] Karla Adam, "How U.K. intelligence came to tweet the lowdown on the war in Ukraine," *The Washington Post*, April 22, 2022, https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/.

[18] UK Ministry of Defence (@DefenceHQ), "The illegal and unprovoked invasion of Ukraine is continuing. The map below is the latest Defence Intelligence update on the situation in Ukraine – 15 May 2023. Find out more about the UK government's," Twitter (renamed as X), May 1, 2023, 6:15 a.m., https://twitter.com/DefenceHQ/status/1658053375961825283.

[19] Walter R. Fisher, "Narration as a human communication paradigm: The case of public moral argument," *Communication Monographs* 51, no. 1 (1984): 1–22.

[20] Hayoung Song et al., "Cognitive and Neural State Dynamics of Narrative Comprehension," *Journal of Neuroscience* 41, no. 43 (October 2021): 8972-8990, https://pubmed.ncbi.nlm.nih.gov/34531284/.

[21] Song et al., "Cognitive and Neural State Dynamics of Narrative Comprehension."

[22] James Wright, "Overcoming political distrust: the role of 'self-restraint' in Japan's public health response to COVID-19," *Japan Forum* 33, no. 4 (2021): 453-475, https://www.tandfonline.com/doi/full/10.1080/09555803.2021.1986565.

[23] Brian Hioe, "Twilight of the Idols: Why We Should Replace the Statue of Chiang Kai-Shek in the CKS Memorial with Zongchai," *The News Lens International*, September 17, 2021, https://international.thenewslens.com/article/156570.

[24] Taiwan Ministry of Health and Welfare (@MOHW_Taiwan), "#衛福編編報報 口發文時間：2022.09.04 新增 34,358 例 COVID-19 確定病例，分別為 34,126 例本土個案及 232 例境外移入 今日新聞稿," Twitter (now renamed X), September 4, 2022, 2:10 a.m., https://twitter.com/search?q=(from%3Amohw_Taiwan) until%3A2022-09-05 since%3A2022-09-03&src=typed_query.

[25] Catherine Porter and Ian Austen, "Justin Trudeau in Home Isolation: 'Daddy's on an Important Phone Call,"' *The New York Times*, March 23, 2020, https://www.nytimes.com/2020/03/23/world/canada/justin-trudeau-coronavirus.html.

[26] Gordon Dow, "Infectious disease specialist uses hockey analogy to describe defence against COVID-19," accessed September 6, 2022, CBC video, 2:44, https://www.cbc.ca/player/play/1720943171570.

[27] M. H. Abrams, *A Glossary of Literary Terms*, 7th ed. (Boston: Heinle & Heinle, 1999).

[28] Northrop Frye, *Anatomy of Criticism: Four Essays* (Princeton, NJ: Princeton University Press, 1957).

[29] CAF Chief of Defence Staff (@CDS_Canada_CEMD), "Conversations on diversity, inclusion, and culture change are not incompatible with our thirst for operational excellence. I count on my senior leaders to champion culture change. Diversity makes us stronger, inclusion improves our institution. We are," Twitter (renamed as X), February 11, 2021, 12:58 a.m., https://twitter.com/CDS_Canada_CEMD/status/1359743611349438464.

[30] Abram Brown, "The Proud Boys Are Furious That Gay Men Have Taken Over #ProudBoys On Twitter," Forbes, October 4, 2020, https://www.forbes.com/sites/abrambrown/2020/10/04/the-proud-boys-are-furious-that-gay-men-have-taken-over-proudboys-on-twitter/.

[31] Canadian Forces in US (@CAFinUS), "#ProudBoys," Twitter (renamed as X), October 4, 2020, 8:40 a.m., https://twitter.com/CAFinUS/status/1312734325104873473.

[32] "DAOD 1002-0, Administration of the Privacy Act," Government of Canada, last modified March 30, 2017, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/1000-series/1002/1002-0-administration-privacy-act.html.

[33] "Policy on Communications and Federal Identity," Government of Canada, last modified August 10, 2019, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30683.

[34] D. H. McKnight and N. L. Chervany, "What is Trust? A Conceptual Analysis and an Interdisciplinary Model," *AMCIS 2000 Proceedings* 382 (2000): 827-833, https://aisel.aisnet.org/amcis2000/382/.

[35] Heidi Tworek, Ian Beacock, and Eseohe Ojo, "Democratic Health Communications during Covid-19: A RAPID Response" (Vancouver: UBC Centre for the Study of Democratic Institutions, September 2020), https://democracy2017.sites.olt.ubc.ca/files/2020/09/Democratic-Health-Communication-during-Covid_FINAL.pdf.

Maintenance Operating Periods in Multi-Domain Operations

Lieutenant Colonel Andrew Bellocchio

The US Army's doctrine is at an inflection point. Adversaries have observed the US Army's reliance on technological dominance, power projection, and sustainment at scale for the past twenty years in Iraq and Afghanistan.[1] Coupled with emerging technologies, strategic competitors such as China and Russia learned to maintain a standoff while gaining an advantage against the US. In response, the US Army is evolving its doctrine to posture for competition in standoffs across multiple domains (land, sea, air, space, cyberspace, and cognitive) and, if needed, to penetrate, disintegrate, and exploit as a member of a joint force (i.e., multi-service) fighting in armed combat. As described by the Army's Training and Doctrine Command (TRADOC), the document requires changes across the elements of doctrine, organization, training, materiel, leadership, personnel, facilities, and policy (DOTMLPF-P).[2]

Doctrine-driven Change to Aviation Sustainment

The *2019 Army Modernization Strategy* provided a framework to transform the army into a multi-domain force by 2035.[3] The strategy highlighted six materiel priorities to drive procurement and modernization, one of which is the Future Vertical Lift (FVL). The FVL platforms will fly further, faster, and longer with greater lethality to increase operational reach and effectiveness against near-peer competitors.[4] The FVL family of systems is the army's next generation of rotorcraft and uncrewed aircraft that will achieve increases in reach, protection, and lethality far greater than the enduring fleet of Apaches, Black Hawks, and Chinooks that were designed in the 1960s and 1970s. Current procurement efforts are scheduled to field Future Attack Reconnaissance Aircraft (FARA), Future Long Range Assault Aircraft (FLRAA), and Uncrewed Aircraft Systems (UAS) in the early 2030s.[5]

As the materiel solution promises advanced aircraft for Multi-Domain Operations (MDO), the sustainment strategy must likewise adapt to the more capable aircraft operating in the new MDO environment. For the last twenty years, army aviation largely sustained itself from the sanctuary of large airfields such as Balad, Bagram, and Kandahar Air Bases. This sustainment approach was logical because the combined allied air forces possessed air supremacy, and the military could take advantage of the US and allies' sustainment scale and capacity.[6] In an MDO environment, however, air superiority is not assured, and a near-peer adversary can threaten large logistical bases; therefore, the US Army must change how it sustains aviation operations in the future.[7]

Meeting Doctrine's Need through Maintenance Free Operating Period (MFOP)

In 2017, TRADOC authored *The U.S. Army Functional Concept for Sustainment* (AFC-S).[8] The sustainment approach stated that "a combination of logistics demand reduction and novel distribution capabilities is essential to enabling multi-domain battle and semi-independent operations."[9] A year later, Lindsay Maples conducted a gap analysis of AFC-S's sustainment

concept.[10] The author found two primary gaps not addressed by the AFC-S: effective sustainment in dispersed operations and under Area Access/Area Denial (A2/AD). *The U.S. Army in Multi-Domain Operations 2028* acknowledged the need for dispersed deployment and sustainment by calling for aviation units to "rotate through a network of dispersed, austere locations in the Tactical Support and Close Areas."[11] Dispersed units functioning as multi-domain formations are recognized as a key part of MDO (Figure 1). A key action for multi-domain formations is to possess the ability to manoeuvre independently, which is partially defined as "operating dispersed for an extended period without continuous [or contiguous] support."[12] (The full definition is in Figure 1.)

To achieve independent manoeuvre and function in austere locations, aviation units must be able to operate for short periods of time with minimal sustainment (e.g., maintenance). Thus, operating periods with no or little maintenance are highly desirable in MDO. Operating for extended periods with no maintenance is a sustainment approach known to reliability engineers as Maintenance Free Operating Periods (MFOP).

MFOP is an attractive sustainment strategy for MDO because it offers an assurance of flight operations over a given number of operating hours that are neither disrupted by maintenance actions nor encumbered by heavy sustainment needs. The similarity between the definitions of independent manoeuvre (Figure 1) and Maintenance Free Operating Period (Figure 2) is noteworthy—the conclusion is that MFOP provides a means for aviation assets to achieve independent manoeuvre.

***Independent Maneuver -- Operating dispersed for an extended period without continuous [or contiguous] support** from higher echelons while retaining the ability to concentrate combat power rapidly at decisive spaces by employing cross-domain fires and maneuver to achieve mission objectives within the intent of the theater campaign.*

Figure 1: Maintenance Free Operating Periods are implied as part of the independent manoeuvre required in Multi-Domain Formations (highlighted in green).
Source: *The U.S. Army in Multi-Domain Operations* (TRADOC Pamphlet 525-3-1).[13]

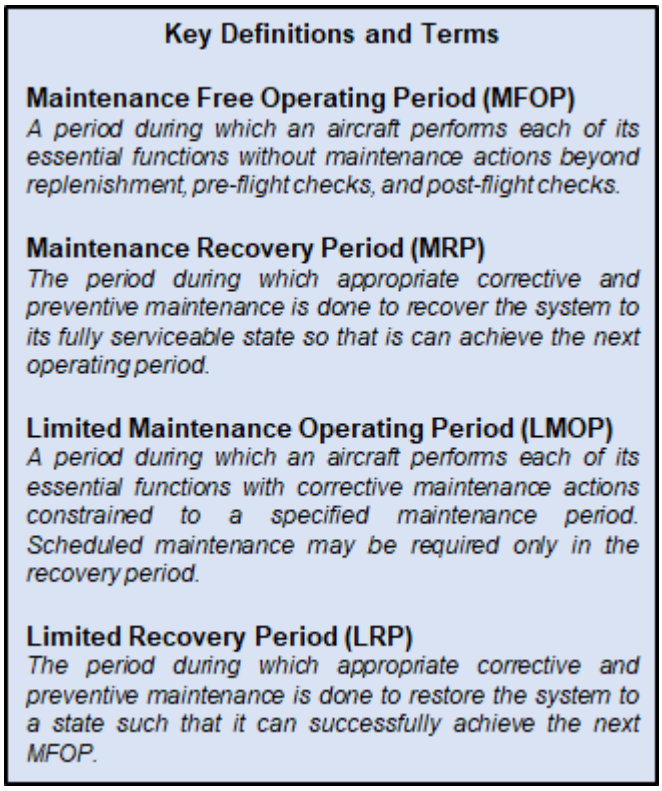

Figure 2: Key Definitions and Terms.
Source: *The U.S. Army in Multi-Domain Operations* (TRADOC Pamphlet 525-3-1).[14]

From Status Quo to Operating Periods

Today's enduring fleet or status quo (see the top concept in Figure 3) experience frequent disruptions to flight operations as the result of maintenance. An MFOP strategy minimizes disruption during the operating period by consolidating all scheduled maintenance (i.e., preventive maintenance based upon a calendar, cycles, or flight time shown as grey in Figure 3) to a recovery period after the completion of the operating period. To help with this consolidation, the US Army is investigating the application of Maintenance Steering Group 3 techniques to synchronize scheduled maintenance into the recovery period.[15]

An MFOP strategy also seeks to minimize the disruption caused by unscheduled maintenance (i.e., unexpected faults discovered in flight or during operation checks, shown as red in Figure 3) through prognostic and predictive maintenance. Prognostics and Predictive Maintenance (PPMx)—shown as blue in Figure 3—have matured after the demonstrated success of conditions-based maintenance and the arrival of technologies such as diagnostics, structural health monitoring, analytics, and artificial intelligence.

Risk-based Maintenance in MFOP

The conceptual framework for maintenance operating periods has two approaches. The strictest interpretation is MFOP, which is highly desired but may not be achievable by FVL. A Limited Maintenance Operating Period (LMOP), discussed later, offers an approach that is practical and achievable by FVL.

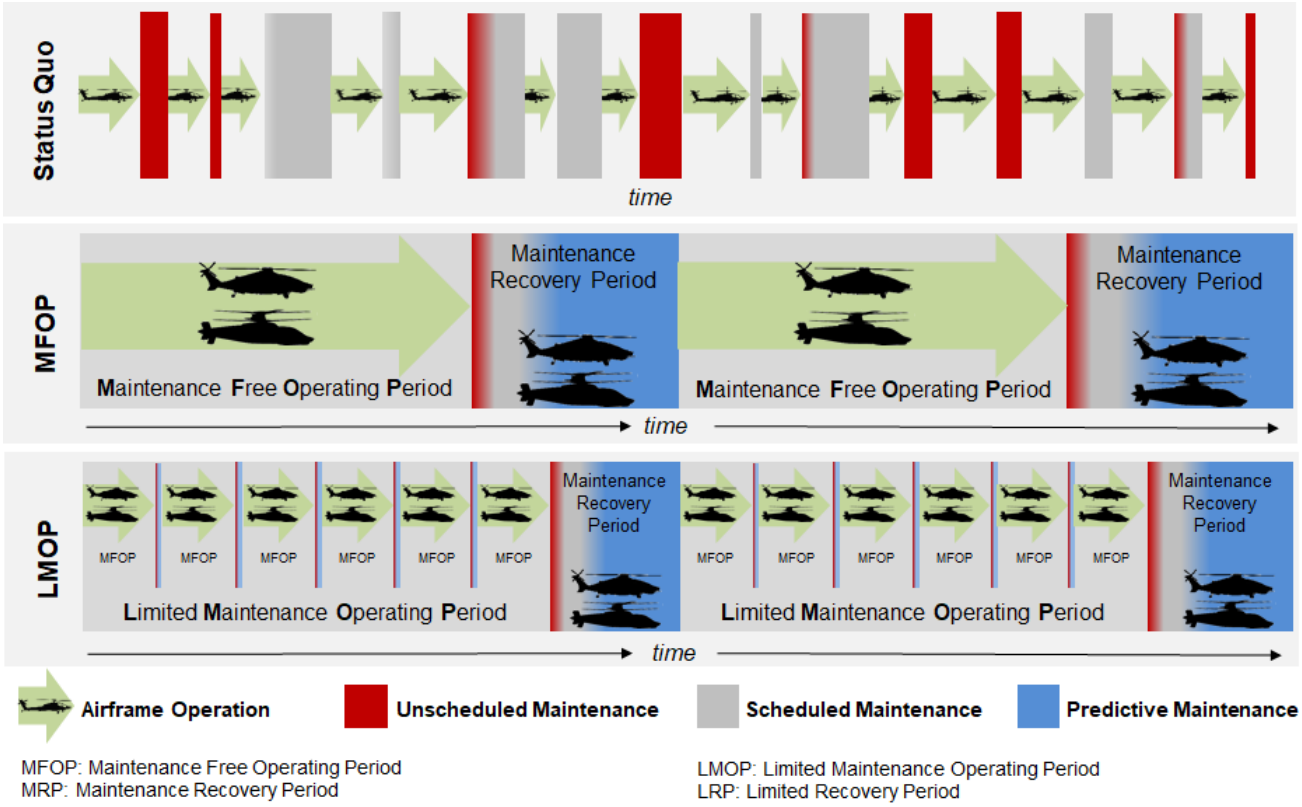

Figure 3: The conceptual framework for maintenance operating periods has two approaches: MFOP or LMOP.
Source: Author

An MFOP is not necessarily maintenance free. Rather, it smartly uses risk-based maintenance to manage maintenance tasks in the recovery period. PPMx anticipates component wear out with sufficient notice to allow repair before disruptive failure occurs. These new technologies and the advent of PPMx support a risk-based maintenance approach. An operating period strategy measures the risk of disruption to the operating period (frequency and repair time) and excessive recovery periods. Consequently, risk-based maintenance "seeks the minimization of failure during the operating period *and* the minimization of the subsequent recovery period duration."[16] Risk-based maintenance provides the commander with the tool to inform maintenance decisions while preserving the operating period. It allows the commander to see which preventive repairs to undertake at the recovery stage to provide the best probability of success for the next operating period.

MFOP shares much with the commercial airline industry's Time-Limited Dispatch (TLD) approach. Airlines dispatch an aircraft for flight operations throughout the day, with maintenance occurring after reaching a time limit measured in flight hours.[17] The main difference between MFOP and TLD is that the latter is based upon short-term fault acceptance, while the former is more comprehensive in its use of multiple approaches to minimize disruption to flight operations.

Impact of Reliability: Today and in the Future

A longer operating period duration is desirable to extend FVL's independent manoeuvre. However, the current and near-term component reliabilities limit the achievable operating period duration. Matthew Beigh et al. estimated the performance of a mature and generic representative utility helicopter (RUH) attempting a 12-hour operating period (shown in Figure 4). The RUH successfully completed the 12-hour period without an essential maintenance action in only 34 per cent of the attempts. The discrete event simulation then explored the impact of near- and future-term reliability in the RUH. Near-term provides a 100 per cent improvement in system reliability and is considered an achievable level by the next generation of rotorcraft, such as FVL. Future-term represents a 500 per cent improvement in reliability and is considered two or more generations away.[18] Sustained maintenance-free operating periods beyond 30 hours appear unlikely for FVL aircraft that are designed today and fielded in the next decade.

Fitting Doctrinal Needs to Achievable Goals Using LMOP

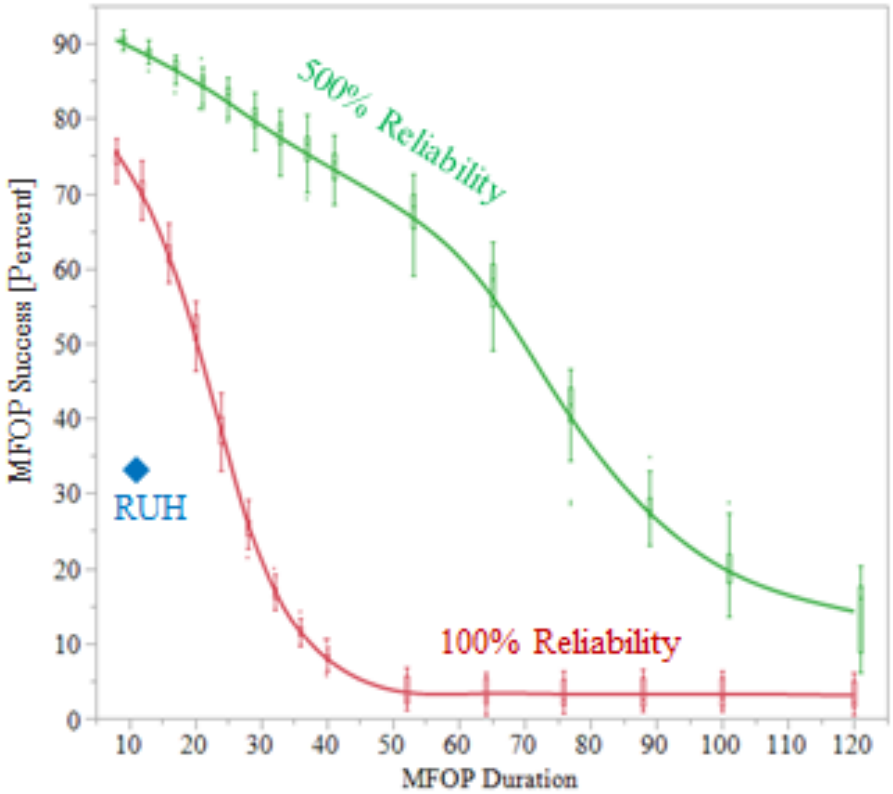

Figure 4: The probability of achieving the MFOP is plotted against an MFOP duration. An RUH is plotted as a diamond. Future solutions are shown with 100% and 500% increases in current reliability. Box plots in quartiles estimate uncertainty.
Source: Beigh et al.[19]

Recognizing that FVL designs are at risk of achieving longer periods, an alternate approach to operating is introduced as LMOP. An LMOP is a series of shorter, maintenance-free operating periods, as sketched in Figure 3. Such shorter bursts of operations align with MDO. The doctrine

specifies independent manoeuvre with a reduced logistics demand to maintain offensive operations over three to four days.[20] LMOP is a means to string together shorter, more achievable MFOPs (fewer than 30 flight hours) that satisfy the need to conduct offensive operations over a few days at a time.

Inside the LMOP and after each shorter MFOP, corrective and preventive maintenance is done in a Limited Recovery Period (LRP). Each LRP is a few maintenance hours and may be done in the tactical support area by organizational maintenance. This concept enables a Progressive Phase Maintenance (PPM) approach by permitting some preventive maintenance in the recovery between MFOPs.

After the conclusion of the LMOP, a full Maintenance Recovery Period (MRP) is performed to prepare the aircraft to achieve the next LMOP. Scheduled maintenance may be done at the LRP at the discretion of the commander but cannot be required. Scheduled maintenance shall be required only in the full maintenance recovery period. This reduces the disruption of scheduled maintenance during the LMOP and empowers the commander to balance mission and maintenance demands.

Shorter MFOPs (fewer than 30 hours) present a lower risk to FVL and facilitate MDO's desire for reduced logistics demand during 72 to 96 hours of offensive operations. LMOP offers a series of shorter MFOPs that support successive offensive operations during MDO's penetrate, disintegrate, and exploit phases. LMOP employs achievable MFOPs while providing the independent manoeuvre required of FVL in MDO. Controlling the LRP decreases the logistical footprint in the tactical assembly areas, making the formation more mobile and survivable against long-range artillery and air threats. Finally, the predictability of the LRP and MRP enables precision logistics required by MDO to provide a reliable, agile, and responsive sustainment capability.

As a new concept, LMOP requires further analysis through modelling and simulation to identify achievable goals that can be quantified in requirements documents. Properly controlling the LRP ensures the advantages gained by independent manoeuvre are not overcome by excessive maintenance. Repairs in the LRP should have a short duration (less than an hour) and require minimal parts, tools, and expertise. Allowable maintenance actions must be identified and designed for the LRP, while all other actions are restricted to the longer MRP. Finally, the impact of forward maintenance on sparing levels and throughput of sub-assembly repairs at the depot requires further study.

Time for Change to Operating Periods

The British Royal Air Force introduced MFOP in the 1990s as part of the Ultra Reliable Aircraft Pilot study.[21] The study achieved limited success because of immature technologies and limits on existing aircraft. In 2011, NATO's AVT-144 Technical Team concluded that new aircraft designs incorporating emerging technologies are needed to fully realize the benefits of MFOP.[22] FVL presents the US Army with its first chance to make that revolutionary leap in maintenance.

The combination of new doctrine and the arrival of the next-generation rotorcraft is a unique opportunity for the proposed change. Approaches like risk-based maintenance and technologies such as health-monitoring systems are now mature enough to begin shorter operating periods under the LMOP concept. LMOP achieves the desired independent manoeuvre to meet MDO's need for between 72 to 96 hours of offensive operations. As FVL matures in later increments, the operating period duration will likely grow and begin to resemble a traditional MFOP. Thus, MFOP sits at the intersection of a doctrinal need and the opportunity provided by

the FVL family of systems as a new platform capable of using maturing technologies. FVL is the moment for change to operating periods.

About the Author

Lieutenant Colonel **Andrew Bellocchio** is an Associate Professor and Academy Professor in the Department of Civil & Mechanical Engineering, United States Military Academy. He holds a Bachelor of Science degree in Mechanical Engineering from West Point and earned a Master of Science (2005) and a Ph.D. (2018) in Aerospace Engineering from the Georgia Institute of Technology. He is a Senior Aviator and has flown rotorcraft and fixed-wing aircraft. LTC Bellocchio currently serves as Director of the United States Military Academy's Center for Innovation and Engineering to facilitate cadet and faculty research. His research interests are in aircraft reliability and structural health monitoring.

Disclaimer

The views expressed herein are those of the authors and do not purport to reflect the position of the United States Military Academy, the US Department of the Army, or the US Department of Defense.

Acknowledgements

Portions of this research were funded by US Army Futures Command. This is a work of the US Government and is not subject to copyright protection in the US. This work is approved for public release.

Endnotes

[1] U.S. Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (2018), https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf, i.

[2] TRADOC, TRADOC Pamphlet 525-3-1.

[3] Michael A. Grinston, James C. McConville, and Ryan D. McCarthy, *2019 Army Modernization Strategy: Investing in the Future* (2019), https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.

[4] Grinston, McConville, and McCarthy, *2019 Army Modernization Strategy*, 6.

[5] U.S. Army Program Executive Office Aviation, "Forging the Future of Army Aviation" (2022), https://api.army.mil/e2/c/downloads/2021/12/21/8f4c1ef1/peo-avn-fy22-strategic-plan-reduced-v11.pdf.

[6] Mark A. Milley, foreword to TRADOC Pamphlet 525-3-1, by TRADOC.

[7] On air superiority, see Department of the Army, *Field Manual (FM) 3-0 Operations* (Washington, DC: Headquarters, Department of the Army, 2022), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.

[8] TRADOC, TRADOC Pamphlet 525-4-1, *The U.S. Army Functional Concept for Sustainment 2020-2040* (2017), https://adminpubs.tradoc.army.mil/pamphlets/TP525-4-1.pdf.

[9] TRADOC, TRADOC Pamphlet 525-4-1, iii.

[10] Lindsay S. Maples, "Sustainment Considerations for the Multi-Domain Battle" (Master's thesis, School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2018), https://apps.dtic.mil/sti/citations/AD1071756, 1.

[11] TRADOC, TRADOC Pamphlet 525-3-1, 37.

[12] TRADOC, TRADOC Pamphlet 525-3-1, GL-5.

[13] TRADOC, TRADOC Pamphlet 525-3-1, v, GL-5.

[14] TRADOC, TRADOC Pamphlet 525-3-1, v, GL-5.

[15] Abdel-Moez Bayoumi, Rhea Matthews, and Evan Barnett, "Advancement of U.S. Army Maintenance Practices for Rotorcraft using MSG Techniques," *Vertical Flight Society's 77th Annual Forum Proceedings* (2021): 7-9, https://doi.org/10.4050/F-0077-2021-16849.

[16] Andrew Bellocchio, Kathryn Pegues, and Steven Chetcuti, "Product Support in a Maintenance Free Operating Period Strategy," *Proceedings of the 77th Annual Forum of the Vertical Flight Society* (2021): 5, https://doi.org/10.4050/F-0077-2021-16848.

[17] Darren Prescott and John Andrews, "Modelling the Use of Maintenance to Minimise Aircraft Service Disruption, *IFAC Proceedings Volumes* 43, no. 3 (2010): 44–45, https://doi.org/10.3182/20100701-2-pt-4012.00009.

[18] Matthew Beigh et al., "Modeling a Maintenance Free Operating Period Strategy for Future Vertical Lift," *Vertical Flight Society 76th Annual Forum Proceedings* (2020): 1-8, https://doi.org/10.4050/F-0076-2020-16270.

[19] Beigh et al., "Modeling a Maintenance Free Operating Period Stratgy for Future Vertical Lift," 8.

[20] TRADOC, TRADOC Pamphlet 525-3-1, 44.

[21] Christopher Hockley and David Appleton, "Setting the requirements for the Royal Air Force's next generation aircraft" (presentation, Annual Reliability and Maintainability Symposium, Philadeliphia, PA, January 13-16, 1997), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=571662.

[22] Graeme F. Eastaugh et al., *Enhanced Aircraft Platform Availability Through Advanced Maintenance Concepts and Technologies*, RTO Technical Report (TR-AVT-144) (Research and Technology Organisation, NATO, 2011), https://apps.dtic.mil/dtic/tr/fulltext/u2/a545816.pdf, 5-59, 6-118.

Investigation of Ground-Based Air Defence System Options Using Simulation and Data Farming

Maude Amyot-Bourgeois, George Nikolakakos, and Lynne Serré

The "grey zone" refers to a set of operations between competitors (state and non-state actors) that are more intense than peacetime diplomacy but characterized by conflicts below the threshold of conventional warfare.[1] The types of operations conducted in the grey zone extend beyond kinetic actions, venturing into diplomatic, informational, and economic territories. Notably, the highest level of intensity remains the military actions against competitors that might not be met with a declaration of war, but that may strain resources and leak intelligence, as experienced by the Taiwanese Air Force against its Chinese competitor.[2] In other examples, Iran and Israel have accused one another of conducting drone and missile strikes against oil tankers and commercial ships.[3] And two Saudi Aramco oil facilities were attacked in 2019 by drones and missiles, which momentarily disrupted the country's oil industry.[4] Domestically, Canadian and American Arctic airspace has been regularly challenged by Russian bombers and surveillance aircraft in recent years.[5] A common theme among these recent grey zone operations has been the use of airborne threats.

As airborne threats, such as missiles, rocket, artillery, and mortar (RAM) munitions and drone technology, have become accessible to an increasing number of state and non-state actors, it has become progressively vital that the Canadian Army acquires a Ground-Based Air Defence (GBAD) capability to protect its land-force elements and key installations against airborne attacks.[6] The Canadian Army GBAD requirements have been assessed, and potential architectures have been studied.[7] Additionally, the performance of a select number of systems considered for the future Canadian GBAD capability has been previously examined by Defence Research and Development Canada (DRDC) Valcartier Research Centre using high-fidelity modelling and simulation. In this paper, we build on their previous work by applying their calculated kill probabilities as a function of range and target type, obtained through individual performance assessment modelling, to a broader modelling and simulation study involving multiple systems and threats. More specifically, data farming methods are used to compare the performance of various GBAD system options against airborne threats in the context of a point-defence scenario.

The paper is organized as follows. The following section describes the methodology applied to conduct the GBAD options assessment. This includes a brief description of data farming, the modelling process that was applied using an agent-based modelling tool called Map Aware Non-uniform Automata (MANA), which was developed by the New Zealand Defence Technology Agency, and the design of the experiment used. The subsequent section reports on the experimental results obtained. The final section concludes the paper by describing the significant findings and suggesting areas for further study.

Methodology

The experiment performed for the assessment of the GBAD systems followed a process called data farming. This concept was first proposed in 1997 and developed through the Project Albert working group, affiliated with the US Marine Corps.[8] Its usage for military applications was further investigated by various NATO modelling and simulation task groups (MSG-088, MSG-124, MSG-

155), resulting in the publication of several comprehensive reports on the process.[9] The US Naval Postgraduate School SEED Center for Data Farming has also produced numerous theses and papers on the subject.[10] Data farming emerged from the rapidly increasing performance of computers that allowed for the generation and storage of massive amounts of data, combined with the desire to explore data smartly and efficiently (to grow and harvest in data-farming terms), which could be used to answer specific questions.

Data farming is an iterative process in which a preliminary analysis is followed by the growth of additional data in interesting regions of the explored parametric space. Trend predictions, explanations of outcomes and outliers, and many more insights can be extracted from the data generated.[11] The DRDC's Centre for Operational Research and Analysis (DRDC-CORA) has recently developed a capacity to utilize the data farming concept for procurement investigations and other military applications.[12] The following subsections detail the steps of the GBAD study that correspond to the data farming process.

Air Defence Scenario

An air defence scenario was developed within the MANA simulation environment to assess the performance of different GBAD systems against various key threats. The scenario was inspired by a previous tabletop exercise conducted by the DRDC Counter Uncrewed Aerial Systems (CUAS) working group. That study investigated the defence of a vital point, where a forward-deployed activity was being conducted against threats from hostile Uncrewed Air Vehicles (UAVs). In the present study, the vital point (or high-value asset) being defended is an airfield. RAM munitions of varying sizes and intensities, as well as a swarm of UAVs of varying numbers, are targeting the airfield, which is being defended by different GBAD system concepts that are considered for this study. The overall aim of the experiment is to assess the performance of the competing GBAD systems against the various key threats.

Model Development

The modelling of the point-defence scenario was implemented using MANA.[13] MANA is a relatively simple and abstract two-dimensional distillation tool, making it well suited for data farming studies. As a result of the high level of abstraction, only the horizontal component of the threat trajectories was considered in this study. The interaction between the threats and the effectors was simplified to the kill probability (i.e., the probability of the outbound intercepting effector defeating and incapacitating an incoming threat) as a function of the distance depending on the type of threat and the type of effector. It was further assumed that an effector engagement was limited to one target at a time. The kill probabilities used in this study were extracted from three different high-fidelity GBAD performance assessment studies produced by DRDC Valcartier Research Centre and calibrated for MANA. Four RAM threats were modelled: 81 and 120 mm mortars, 155 mm artillery rounds, and 220 mm rockets. Each threat type was assigned a trajectory characterized by speed and maximum projectile range. The UAV modelling was based on the specifications of a small NATO Class 1 UAV. The terrain aspect, as well as the environmental conditions, were not considered for this investigation. The GBAD sensor system was assumed to be perfect, focusing the study only on the effector-threat engagements. Figure 1 illustrates the initial position of each entity for the RAM case and the positions of the modelled GBAD systems: the Iron Dome, Centurion, and the targeted airfield.

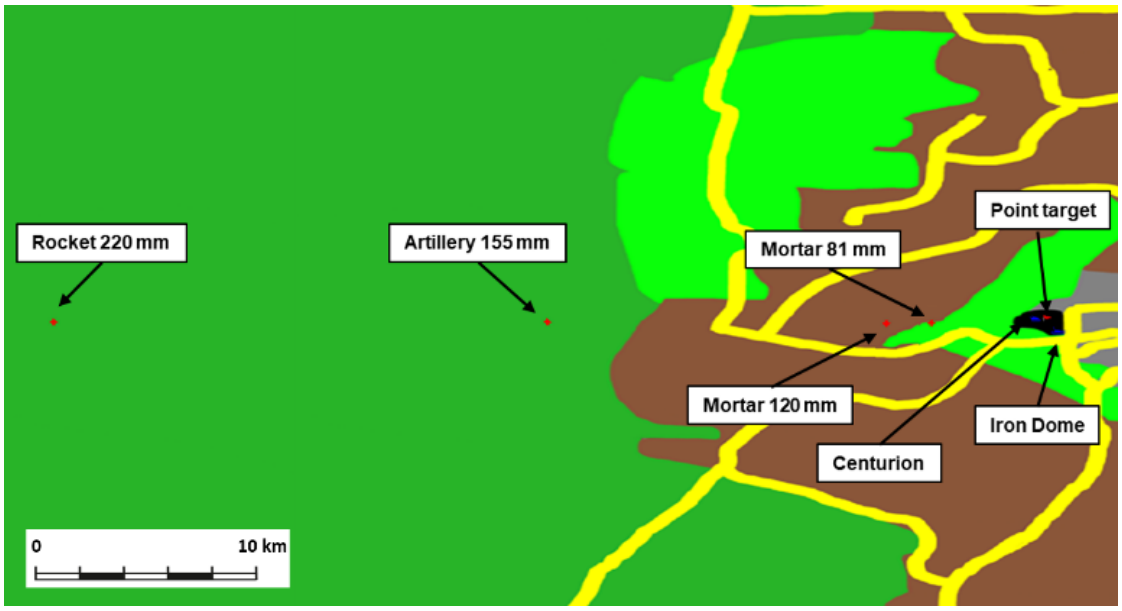

Figure 1: Map at the start of an iteration for the RAM scenario.
Source: Authors

Design of Experiment

Among the independent variables, four variables of interest were parameterized in scenario 1 (RAM): the GBAD system type, the threat type, the number of threats, and the threat-launching rate. The GBAD systems considered included a medium-range, missile-based interceptor, a short-range, gun-based interceptor (based on the Centurion, the land-based version of the Close-In Weapon System [CWIS]), and a combination of the two systems. The threat-launching rate was defined as the number of threats launched per minute. For scenario 2 (UAV swarm), two variables of interest were selected: the GBAD system type and the UAV swarm size (i.e., the number of inbound UAVs). Here, two potential future High-Energy Laser (HEL) systems and their combinations with the Iron Dome-based or Centurion-based system were added to the list of GBAD systems under consideration.

Table 1 captures the range and increments of the sampling applied for each parameter, or the possible levels for the categorical variables. Other independent variables, such as the initial positions of the threats and GBAD systems, the ammunition load, the delay between two missile shots (Iron Dome) or two salvoes (Centurion), and the illumination dwell time (HEL) of each system were kept constant throughout the experiments.

Parameter	**Levels (categorical); or range and increment (discrete quantitative)**
Scenario 1: RAM threats	
GBAD system/mix (3)	Iron Dome; Centurion; Iron Dome + Centurion
Threat type (4)	Artillery 155mm; Mortar 81mm; Mortar 120mm; Rocket 220mm
Threat number	[8, 15]

Threat launching rate	Range: [1 – 30]; Increment: 1; Unit: [threats/min]
Scenario 2: UAV Swarm	
GBAD system/mix (9)	Iron Dome; Centurion; 5 kW HEL; 30 kW HEL; Iron Dome + Centurion; Iron Dome + 5 kW HEL; Iron Dome + 30 kW HEL; Centurion + 5 kW HEL; Centurion + 30 kW HEL
UAV swarm size	[1, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50]

Table 1: Description of the range of values for the variables of interest.
Source: Authors

The design points (DPs) were generated following the factorial design of the experiment method, which means that every possible combination of the different values for each parameter was included. Five hundred iterations per DP were respectively performed for the RAM and UAV swarm scenarios, for a total of 360,000 and 49,500 data points collected for each case. The simulations were run in batch mode using the command line interface to maximize processing speed and efficiency.

Measure of Performance

The raw data files collected from each data point contain information on the status of the threats (dead or alive), their shooter identity, the position of death, and the ammunition usage for the GBAD systems. The raw files were organized into a table in which each row was associated with an iteration of a particular DP. They contained information on all the parameters and measures of performance (MOP) and measures of effectiveness (MOE) that were of interest to the investigation. This compilation of results was then used for the post-simulation analysis. In this paper, the analysis is limited to one MOE, called the probability of raid negation (P_{raid}), which represents the probability that the GBAD system will intercept all threats for a given DP, thus allowing no threat leaks to the target. A particular data point is given a binary value N_{raid}, set at 1 for iterations where the GBAD system negated all threats and 0 otherwise. The P_{raid} is then obtained by averaging N_{raid} over the 500 replications.

Results and Analysis

Figure 2 displays the results of the scenario 1 experiment (RAM threats). P_{raid} is plotted as a function of the RAM threat rate with 95 per cent point-wise confidence intervals for each of the three GBAD system options against the four different threat types. The number of inbound threats was either eight (thin line) or fifteen (thick line).

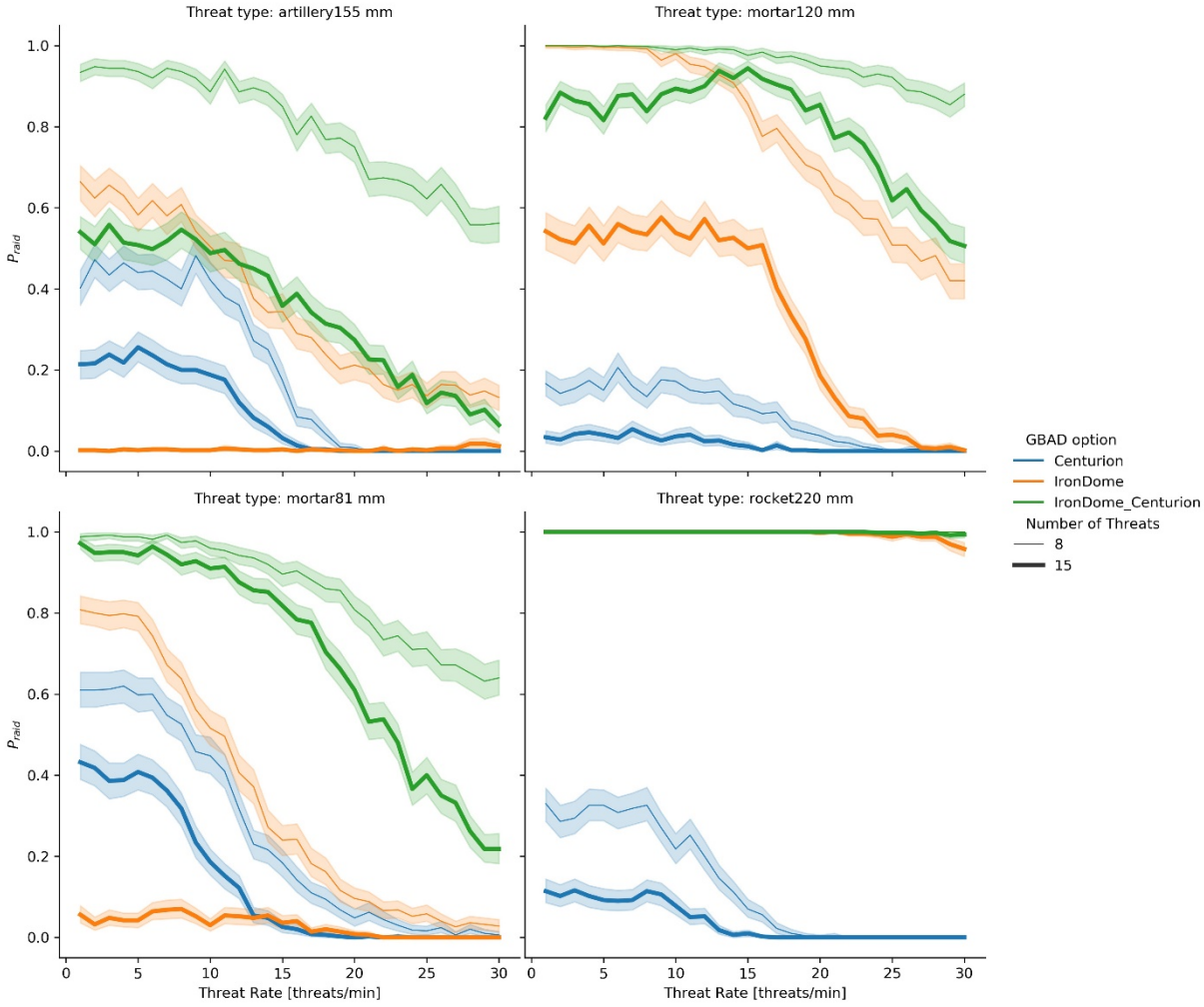

Figure 2: Probability of raid negation for scenario 1 (RAM threats) versus the three GBAD system options.
Source: Authors

Figure 2 shows that, in general, P_{raid} diminished as the number of incoming threats increased from eight to fifteen, as the GBAD system became overwhelmed. Similarly, as the threat-launching rate increased, P_{raid} decreased. Some cases, such as Iron Dome or Centurion against eight 81 mm mortars, exhibited a steep decrease. Others resulted in a much more gradual slope, as was observed for the Iron Dome and Centurion combined systems against eight 120 mm mortars and 155 mm artillery rounds. A notable exception was the case of GBAD system options that included the Iron Dome against 220 mm rockets. In this case, the only scenario where the GBAD system had a $P_{raid} < 1$ was for a lone Iron Dome system against the highest number of rockets and the highest threat-launching rates. This high success rate was attributed to the high kill probability of the Iron Dome system against rockets. The inversion in performance observed between the Iron Dome and Centurion options, when the threat number was increased from eight to fifteen 81 mm mortars, could be explained by relating the threat casualties to the number of remaining ammunition rounds. This shows that the Iron Dome ran out of ammunition as the number of 81 mm threats increased.

Figure 3 displays the results of the scenario 2 UAV experiment. P_{raid} is shown as a function of the UAV swarm size with 95 per cent point-wise confidence intervals for the nine GBAD system options.

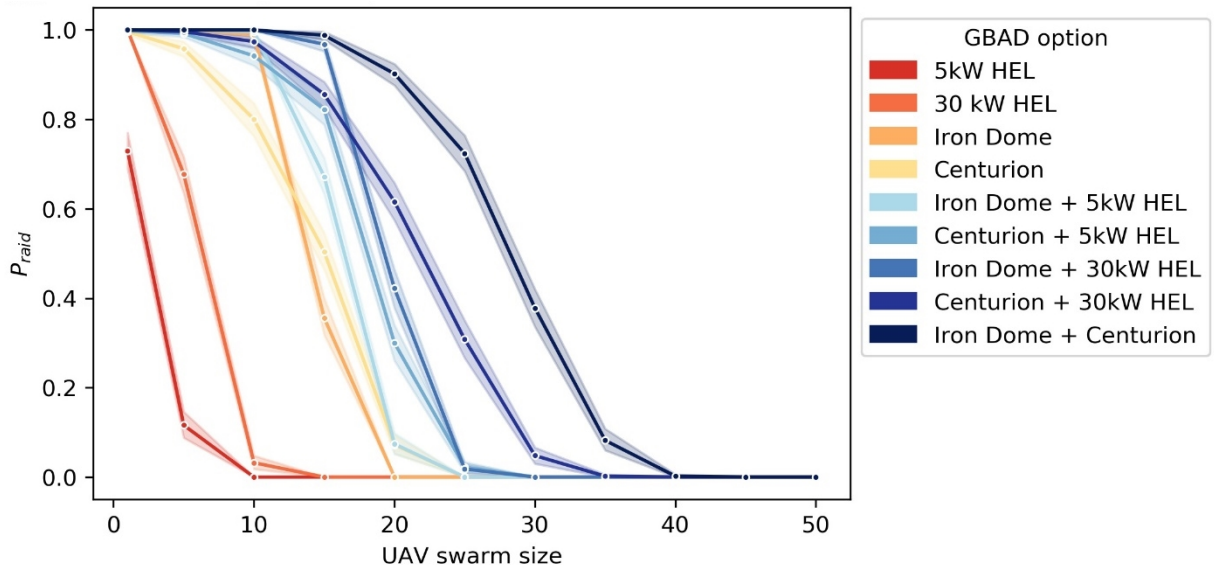

Figure 3: Probability of raid negation for the UAV swarm scenario.
Source: Authors

Figure 3 demonstrates a clear divide in performance between the individual (orange hues) and mixed (blue hues) system concepts, with the latter outperforming the former. The two HEL options were rapidly overwhelmed as the UAV swarm size increased. This was due to the delay between consecutive laser shots, which was longer when compared to the other two GBAD systems under consideration. The top-performing GBAD system option was found to be the mixed system composed of the Iron Dome and Centurion. This combination showed a capacity to negate raids of fifteen or fewer UAVs, with decreased performance becoming apparent as the ammunition load was depleted when swarm sizes were larger.

Conclusion

The study aimed to assess the performance of different GBAD system options against various airborne threats in a point-defence scenario. The probability of raid negation was selected as a measure of performance. It was found that for all of the threat types investigated, as the scenario intensity was increased to test the saturation point of the GBAD system options, the individual systems were overwhelmed more rapidly than the mixed systems. This demonstrated that a mixed system GBAD concept could be more effective than a single-system concept for defending against RAM and UAV threats in a point-defence scenario.

The data farming process using MANA that was developed and applied to this investigation allows for a wider list of variables to be parameterized in future experiments. This includes the delay between shots, the GBAD components' position, and the number of individual systems included. A broader variety of air-defence scenarios, such as a convoy or the protection of the largest possible area occupied by a Canadian Mechanized Brigade Group, is also of interest for future work.[14] Increasing the number of parameters being explored will render the analysis via

summary statistics and visualization much more complex. To overcome this, DRDC-CORA has been developing machine-learning methods that support the analysis and will be applying them to interpret the results. The P_{raid} analysis offered a good general overview of system performance but was insufficient to understand and extract all relevant system trends and performance information. A broader range of MOP will be considered in future experiments to complement the P_{raid}, such as the percentage of threats intercepted, the number of ammunition used, and ammunition efficiency.

About the Authors

Maude Amyot-Bourgeois is a defence scientist with Defence Research and Development Canada's Centre for Operational Research and Analysis. Since 2019, she has worked in collaboration with her colleagues from the Canadian Army Operational Research and Analysis Team on various combat simulation studies. She obtained her master's degree in physics from the University of Ottawa. Her email address is maude.amyot-bourgeois@forces.gc.ca.

Dr. **George Nikolakakos** is a defence scientist with Defence Research and Development Canada's Centre for Operational Research and Analysis. Since 2019, he has worked in collaboration with colleagues from the Canadian Army Operational Research and Analysis Team on various combat simulation studies. He obtained his Ph.D. in physics from York University. His email address is george.nikolakakos@forces.gc.ca.

Lynne Serré first joined Canada's Department of National Defence in 2013 as a defence scientist under Director General Military Personnel Research and Analysis, where she specialized in military workforce modelling and analysis. In 2019, she joined Defence Research and Development Canada's Centre for Operational Research and Analysis, providing support to the Canadian Army headquarters in Ottawa. Since 2021, her research has been focused on topics related to air defence. She obtained her master's degree in computational mathematics from the University of Waterloo. Her email address is lynne.serre@forces.gc.ca.

Acknowledgements

The authors would like to thank Major Marie-Christine Alamy (formerly) from the Canadian Army Land Warfare Centre; Richard Lestage, Eric Gagnon, and Jean-Francois Daigle from DRDC-Valcartier; as well as Bao Nguyen from DRDC-CORA for providing useful advice to orient this research.

Endnotes

[1] Philip Kapusta, "The Gray Zone," *Special Warfare* 28, no. 4 (October-December 2015): 18-25; Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80, no. 1 (2016): 101-109, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/article/643108/unconventional-warfare-in-the-gray-zone/.

[2] Yimou Lee, David Lague, and Ben Blanchard, "China launches 'gray-zone' warfare to subdue Taiwan," *Reuters*, December 10, 2020, https://www.reuters.com/investigates/special-report/hongkong-taiwan-military/.

[3] "Vessel owned by Israeli company attacked off UAE coast," *Al Jazeera*, April 14, 2021, https://www.aljazeera.com/news/2021/4/14/vessel-owned-by-israeli-company-attacked-off-uae-coast-reports; "Oil tanker off Syrian coast hit in suspected drone attack," *Al Jazeera*,

April 24, 2021, https://www.aljazeera.com/news/2021/4/24/oil-tanker-off-syrian-coast-hit-in-suspected-drone-attack; Kareem Fahim and Shira Rubin, "U.S., Britain, Israel blame Iran for fatal drone strike on oil tanker; Tehran denies responsibility," *The Washington Post*, August 1, 2021, https://www.washingtonpost.com/world/middle_east/iran-israel-tanker-attack/2021/08/01/d48bae2e-f2bf-11eb-a636-18cac59a98dc_story.html.

[4] David Reid, "Saudi Aramco reveals attack damage at oil production plants," *CNBC*, September 21, 2019, https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html.

[5] Lee Berthiaume, "2 Russian bombers approached Canadian airspace in Arctic, Norad says," *Global News*, January 31, 2020, https://globalnews.ca/news/6489830/russian-bombers-canada-norad/; Tom Roeder, "NORAD chases Russian bombers off; biggest Arctic showdown in years," *The Gazette*, accessed September 3, 2021, https://gazette.com/military/norad-chases-russian-bombers-off-biggest-arctic-showdown-in-years/article_65a7dbda-e952-11ea-aec0-9fc47acf0df4.html; Levon Sevunts, "U.S. homeland defence strategy underlines Canada's importance," *Radio Canada International*, August 28, 2020, https://www.rcinet.ca/en/2021/03/20/usnorthcom-norad-strategy-canada/.

[6] Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

[7] National Defence, "Business Case Ground-Based Air Defence," C.001420 (2019); Jean-Pierre Bourque and Philippe Gouin, "Ground Based Air Defence System Architecture Investigation," Defence Research and Development Canada, DRDC Valcartier CR-2011-106 (February 2013).

[8] Alfred Brandstein and Gary E. Horne, "Data Farming: A Meta-technique for Research in the 21st Century," in *Maneuver Warfare Science 1998*, eds. F.G. Hoffman and Gary E. Horne (US Marine Corps Development Command, 1998), 93-99, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi1ksSpoZv_AhUMq4kEHT_sCPoQFnoECAgQAQ&url=http%3A%2F%2Funbox.org%2Fall%2Ftrunk%2Fdoc%2F06%2FdataFarming%2Fdata_farming.pdf&usg=AOvVaw11g-zeTKOP8qnDv0RYSA9t; Gary E. Horne, "Maneuver Warfare Distillations: Essence not Verisimilitude," in *Proceedings of the 1999 Winter Simulation Conference*, eds. Phillip A. Farrington et al. (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 1999), 1147-1151, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=816833; Gary E. Horne, "Beyond Point Estimates: Operational Synthesis and Data Farming," in *Maneuver Warfare Science 2001*, eds. Gary E. Horne and Mary Leonardi (US Marine Corps Development Command, 2001), 1-7, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=eb1c203e6d8c6d3a1e4922fe04ae8c8fd4006919; Gary E. Horne and Theodore E. Meyer, "Data Farming: Discovering Surprise," in *Proceedings of the 2005 Winter Simulation Conference* (2005), eds. Michael E. Kuhl et al. (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2005), 1082-1087, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1574362.

[9] North Atlantic Treaty Organization (NATO), *Data Farming in Support of NATO*, STO-TR-MSG-088 (Science and Technology Organization, NATO, 2014), https://apps.dtic.mil/sti/pdfs/ADA604058.pdf; NATO, *Developing Actionable Data Farming Decision Support for NATO*, STO-TR-MSG-124 (Science and Technology Organization, NATO, 2018), https://apps.dtic.mil/sti/pdfs/AD1062145.pdf; Daniel Huber et al., "Data Farming services: micro-services for facilitating data farming in NATO," in *Proceedings of the 2019 Winter Simulation Conference*, eds. N. Mustafee et al. (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2019), 2455-2466, http://doi.org/10.1109/WSC40007.2019.9004823.

[10] Susan Sanchez, "Work Smarter, not Harder: Guidelines for Designing Simulation experiments," in *Proceedings of the 2006 Winter Simulation Conference*, eds. L. Felipe Perrone et al., (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2006), 47-57, http://doi.org/10.1109/WSC.2006.323037.

[11] Gary Horne and Klaus-Peter Schwierz, "Summary of Data Farming," *Axioms* 5, no.1 (2016): 1-19, https://doi.org/10.3390/axioms5010008.

[12] Maude Amyot-Bourgeois, Lynne Serré, and Peter Dobias, "Use of Agent-Based Modeling and Data Farming for the Army ISR Capability Assessment," in *Proceedings of the 14th NATO Operations Research and Analysis Conference* (Science

and Technology Organization, NATO, 2020), https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-OCS-ORA-2020/MP-SAS-OCS-ORA-2020-EDT-03-1.pdf; Lynne Serré, Maude Amyot-Bourgeois, and Brittany Astles, "Use of Shapley Additive Explanations in Interpreting Agent-Based Simulations of Military Operational Scenarios," in *Proceedings of the 2021 ANNSIM Conference*, eds. Cristina Ruiz Martin et al., (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2001), http://doi.org/10.23919/ANNSIM52504.2021.9552151.

[13] For more information on MANA, see Gregory C. McIntosh et al., *MANA (Map Aware Non-Uniform Automata) version 4 user manual* (Defense Technology Agency, Auckland, New Zealand, Tech. Note 2007/3 NR1465, 2007); Mark A. Anderson, "Agent-Based Modelling in the New Zealand Defence Force," in Proceedings of the International Defense and Homeland Security Simulation Workshop, eds. Agostino Bruzzone et al. (Rende, Italy: DIME – University of Genova, 2013), 61-66, http://www.msc-les.org/proceedings/dhss/2013/DHSS2013_61.pdf; James R. Williams, "Mathematical Analysis of Algorithms within MANA" (Master's thesis, Naval Postgraduate School, Monterey, California, 2014). For previous DRDC studies using MANA, see Peter Dobias and Cheryl Eisler, "Modeling a Naval Force Protection Scenario in MANA," *Operational Research and Management Science Letters* 1, no.1 (2017): 2-7, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc269/p805239_A1b.pdf; Amyot-Bourgeois, Serré, and Dobias, "Use of Agent-Based Modeling and Data Farming for the Army ISR Capability Assessment"; Serré, Amyot-Bourgeois, and Astles, "Use of Shapley Additive Explanations in Interpreting Agent-Based Simulations of Military Operational Scenarios."

[14] Yazan Qasrawi, "Spatially Bounding a Canadian Mechanised Brigade Group's Operations," Defence Research and Development Canada, DRDC-RDDC-2019-R211 (2019).

GIS Analysis of Potential Missile Targets in Canada Maximizing Potential Damage

Geoff Pond, Emilie Breuvart, Andrew B. Godefroy, and Cindy Lin

While the Cold War may have passed, North America remains at risk from kinetic attacks. The events of 9/11 are a stark reminder that even non-state actors may attempt to cause catastrophic damage in North America, launching strikes from across the globe. Further, state-on-state warfare using conventional kinetic weapons, most recently in Ukraine, has re-established what many thought were outdated Cold War-era threats.[1] This article considers the motivations and means by which state and non-state actors might strike Canada using a ballistic or cruise missile (e.g., policy change, economic damage, regime change), recognizing that contemporary missile technology affords adversaries the opportunity to strike virtually anywhere in the world. Moreover, it considers, with respect to those motivations, what Canadian targets may best meet a potential aggressor's aspirations.

Contemporary Missile Technologies

Intercontinental Ballistic Missiles (ICBMs) have long been the stalwart of deterrents among Cold War actors. Russia and the US have continuously improved on Cold War-era ICBM designs by increasing the lethality of their payloads. For example, beyond just improving a missile's fuel efficiency or payload capacity, designers have maximized the payload delivery with packages containing multiple, independently targetable re-entry vehicles (MIRVs). Specifically, the US continues its development of a ground-based strategic deterrent (GBSD) meant to replace its currently deployed LGM-30G Minuteman III ICBMs. Likewise, Russia is developing the Kedr ICBM to replace the historic RS-24 Yars systems and is hoping to field these weapons by 2030.[2] Notably, the Russians aspire to deploy twenty regiments fielding the Sarmat heavy ICBM by 2030, able to carry the hypersonic boost-glide Avangard re-entry vehicle, thereby imparting Russia the capability of launching from difficult-to-track mobile launchers and to strike virtually anywhere in the globe using a re-entry vehicle travelling at hypersonic speeds. China and India have also introduced new ICBM designs into their arsenals since the end of the Cold War. For example, the recently introduced and tested Chinese DF-ZF hypersonic glide vehicle can be fitted to a variety of existing ballistic missiles. Similarly, the North Korean Hwasong-8 is believed to be of similar design to China's DF-ZF. North Korea's missile test on March 24, 2022 demonstrated a renewed interest in ICBMs and a technological step forward in ICBM technology.[3]

Cruise missiles have also vastly improved in the last two decades. Typically, ballistic missiles have limited manoeuvrability post-launch and are instead committed to following a ballistic trajectory defined primarily by the ascent angle and boost. Following the boost phase of flight, the missile is no longer powered. Conversely, cruise missiles remain powered throughout the entirety of their flight and, consequently, are able to fly at flat trajectories—often at low altitudes—with substantially greater manoeuvrability. The Russians have demonstrated the Zircon anti-ship missile—a hypersonic weapon used for closer-range engagements with naval platforms.[4]

Clearly, notwithstanding the end of the Cold War, the pace of development among ballistic and cruise missiles has not abated. Given the continued advance of these technologies among Cold

War adversaries and others pursuing their own programs (e.g., Iran, China, Pakistan), this pace has only increased.

Belligerent Actor Objectives

Any number of state actors might intentionally launch a missile strike targeting Canada should the situation merit taking such a bold move. Accidental strikes are also conceivable, resulting from targeting errors or mechanical malfunctions as adversaries seek to strike Canada's geographically linked allies (i.e., the US). Certainly, it seems that a nation state would gain little by striking Canada kinetically, given the limited ability of those possessing ICBMs to gain a physical foothold in Canada unless motivated by other objectives. These objectives may include disrupting the economy, isolating Canada from allies, or deterring the political leadership from taking action to defend national interests at home or abroad. Further, supplying and supporting a proxy actor (thereby affording the state actor plausible deniability) and having the opportunity to launch shorter-range weapons (e.g., a short-range containerized missile launcher onboard a maritime vessel offshore) is also conceivable. In such cases, the objectives of the sponsoring state actor may be the same as those noted earlier. One might reasonably question what a non-state proxy actor might have to gain.

Understanding the objectives of non-state actors, their values, and Canada's national priorities is instrumental in optimizing defence resources.[5] Non-state actors engage in kinetic conflicts to pursue goals varying from ultimate (e.g., policy change), strategic (e.g., creation of fear or economic damage), organizational (e.g., morale building), and tactical.[6] It is with these goals in mind that we consider candidate Canadian targets that best achieve them.

The Global Terrorism Database (GTD) is instructive for discerning candidate targets.[7] The GTD contains the details of over 200,000 terrorist attacks throughout the globe collected through the automated natural language processing of millions of news articles published daily, followed by verification by human analysts. This database offers a historical perspective of Canadian sites targeted by non-state actors and how sophisticated weapon systems (e.g., missiles) have been used internationally by non-state actors in pursuit of their organizational objectives. To be included in the GTD, the incident must be intentional and violent. Further, the perpetrators must be "sub-national actors." Lastly, two of the three following criteria must be satisfied: the event falls outside the context of war; the intent was to influence an audience broader than the immediate victims; and the act was perpetrated in pursuit of a "political, economic, religious, or social goal."[8]

Among attacks having occurred strictly within Canada, the GTD includes a total of 106 from 1970 to 2017, perpetrated by domestic and foreign agents, organized groups, and lone wolves.[9] The breadth and distribution of targets reflect the varied objectives of these actors. Those wishing to sow fear might reasonably target the civilian populace, while those seeking to cause economic damage would reasonably target elements of critical infrastructure such as utilities or the transportation grid. They may alternatively target large businesses. Those seeking policy changes may target abortion clinics, government offices, and foreign government missions in Canada.

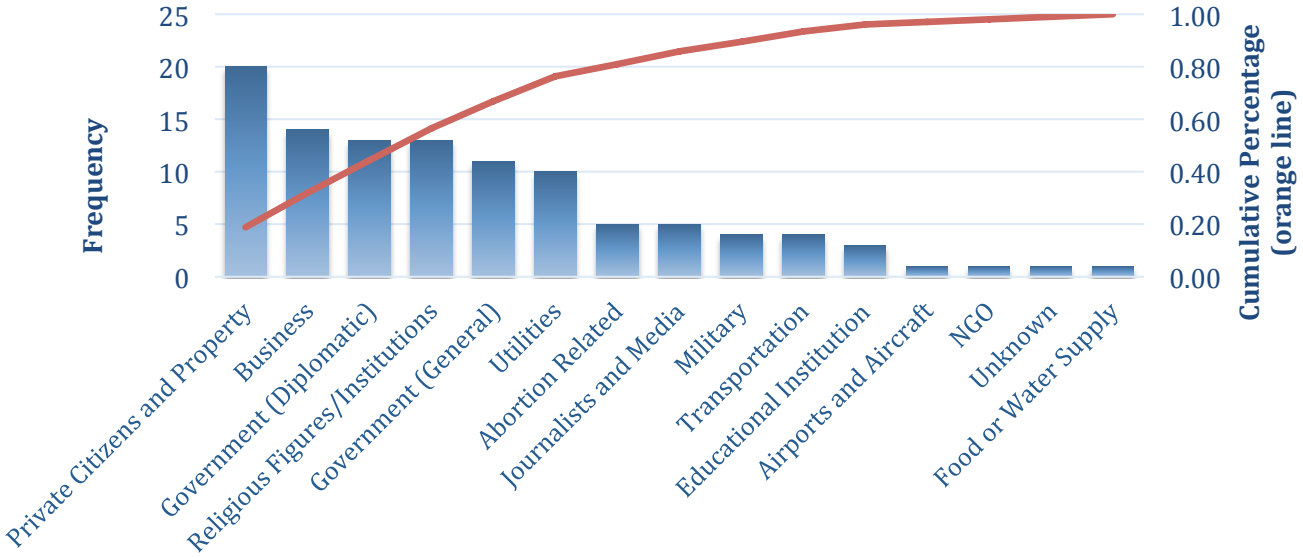

Figure 1: Targets of historical terrorist attacks on Canadian soil.
Source: Authors

Canada also enjoys relative security and stability in comparison to many other nations. Consequently, it may be comparatively easy to strike a diplomatic mission in Canada rather than attacking that nation's government domestically. Such examples include the 1992 attack on the Iranian embassy in Ottawa and the 1985 attack on the Turkish embassy in Ottawa perpetrated by the Armenian Revolutionary Army.[10] The GTD includes thirteen terrorist attacks on international missions in Canada where the target was either high-ranking diplomatic personnel or the embassy building itself. These include targeted attacks against Cuba, Iran, Israel, and Turkey. In only two cases is the perpetrator listed as "unknown." Otherwise, perpetrators of these attacks include Black September (a former Palestinian militant organization), Omega-7 (a historical anti-Castro Cuban group), the Alliance of Revolutionary Cuban Organizations, the Armenian Secret Army for the Liberation of Armenia, the Justice Commandos for the Armenian Genocide, the Armenian Revolutionary Army, and the Anti-Iran Government Exiles.[11] It is also worth noting that Article 22 of the Vienna Convention on Diplomatic Relations (of which Canada is a signatory) obligates Canada to "take all appropriate steps to protect the premises of the mission against any intrusion or damage."[12]

The primary target within the GTD categorized as "utilities" are gas plants. A total of ten domestic events are recorded in the GTD targeting utilities. Only four events are categorized as "transportation"—two of which targeted light-rail systems in either Vancouver or Montreal. While it is tempting to draw comfort from the lack of more recent terrorist attacks in Canada, it is not due to a lack of motivation and initiative among non-state actors. In 2013, individuals plotted and prepared an attack against Via Rail under the guidance and direction of al-Qaeda.[13] The infamous "Toronto 18"—another group affiliated with al-Qaeda—plotted attacks against the Toronto Stock Exchange, Parliament, nuclear power plants, a Canadian Armed Forces base, a CSIS office in Toronto, and the CN Tower in 2006.[14]

The Government of Canada's view of critical national infrastructure offers far more detail on potential targets. Table 1 includes broad categories and more specific sub-categories. In light of

Table 1, a plethora of unprotected targets risks longer-term damage to Canadian communities well beyond the human safety and infrastructure damage under threat as part of the immediate attack.

Sector	**Subcategories**
Energy	Electricity; Nuclear Power; Natural Gas; Petroleum
Finance	Banking; Securities; Insurance; Brokerages
Food	Agri-Supply; Crop Production; Animal Production; Aquaculture; Processing
Government	International; Federal; Provincial; Municipal; Indigenous
Health	Primary Healthcare; Secondary Healthcare; Nursing and Residential Care; Medical Support Services
Information & Communications	Telecommunications; Information Services
Manufacturing	Base Materials; Chemicals; Equipment & Machinery; Technology; Transportation; Pharmaceuticals
Safety	Environment; Incident Response; Community Resilience; Professional Services; Protective Services
Transportation	Air; Marine; Rail; Road; Trucking; Urban
Water	Watershed Management; Potable Water; Wastewater

Table 1: Elements of "critical infrastructure."
Source: Adapted from the Government of Canada.[15]

Among other potential targets, missile systems offer belligerents an opportunity to damage targets without immediate risk to the perpetrator. Historically, in other countries, missiles have been employed by non-state actors to attack targets. Globally, the GTD includes eighty-four events involving "missile(s)" as being among the weapons used.[16] While these attacks occurred predominantly in the Middle East or in Africa, they also include the UK, the US, and other Western nations, spanning from 1978 to 2019. The frequency of each target type among these eighty-four events is depicted in Figure 2. Given the trends, Canada must not assume it remains immune from such adversary tactics.

Based on a review of the GTD, we may conclude that, at least historically, terrorists have preferably targeted private citizens and private property over all other target types when using missiles.[17] Considering all missile attacks in the database, military targets are the second most common target. Government targets (whether legislative or diplomatic) also figure prominently in the dataset.

It is important to note the GTD's definition of terrorism precludes attacks perpetrated by state actors.[18] It would therefore be highly speculative to assume the behaviour, motivations, and intentions of state actors to be represented by the above analysis. Certainly, state actors are far more likely to have access to sophisticated missile systems and have the resources to carry out an attack abroad.

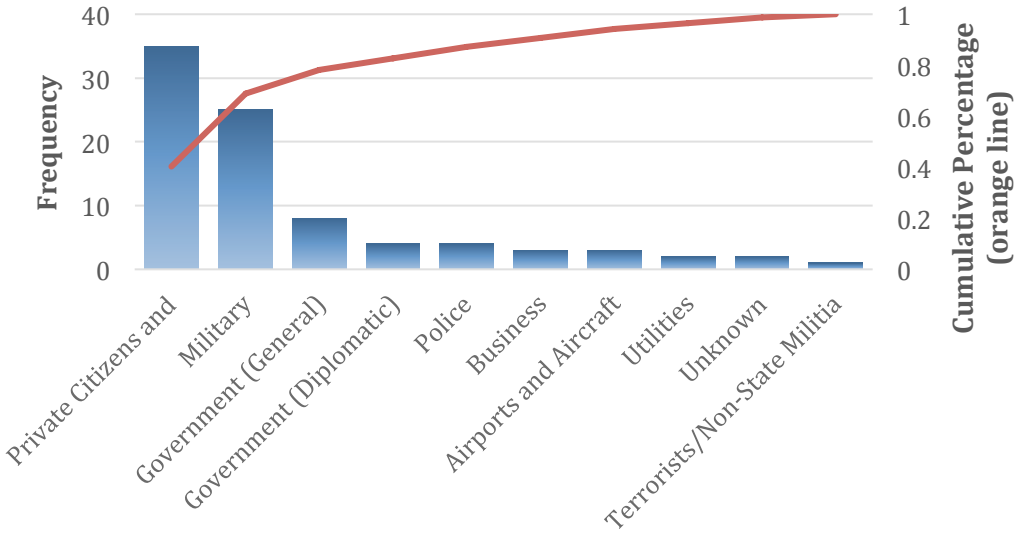

Figure 2: Targets of historical global terrorist strikes among twenty-five countries using missiles.
Source: Authors

Now, considering the breadth of belligerent actor motivations described by Marsden, we have established a list of potential targets.[19] These include areas of high population density to sow fear; areas of substantial commercial, industrial, and private real estate value to cause economic damage; and universities, power plants, hospitals, and specific points of interest, including major sporting venues, government buildings, airports, seaports, and cultural sites. These offer an opportunity for belligerents to pursue objectives varying from policy change, influencing public attitudes, discrediting government, forcing obedience, provoking counter-reactions, and agenda-setting.

We have mapped critical infrastructure and sites of cultural importance across the entire nation and major Canadian cities at higher resolution: Halifax, Quebec City, Montreal, Ottawa, Toronto, and Vancouver using ArcGIS (a geographic information system mapping software).[20] For the list, we combined a variety of datasets provided by Statistics Canada detailing census subdivision boundaries, population density by census subdivision (as established by the 2016 census), property values, locations of post-secondary institutions, and healthcare facilities. These databases were combined with open sources detailing the locations of airports, power-generation plants, refineries, and pipelines. For brevity, we include only Montreal here as an example in Figures 3 and 4.

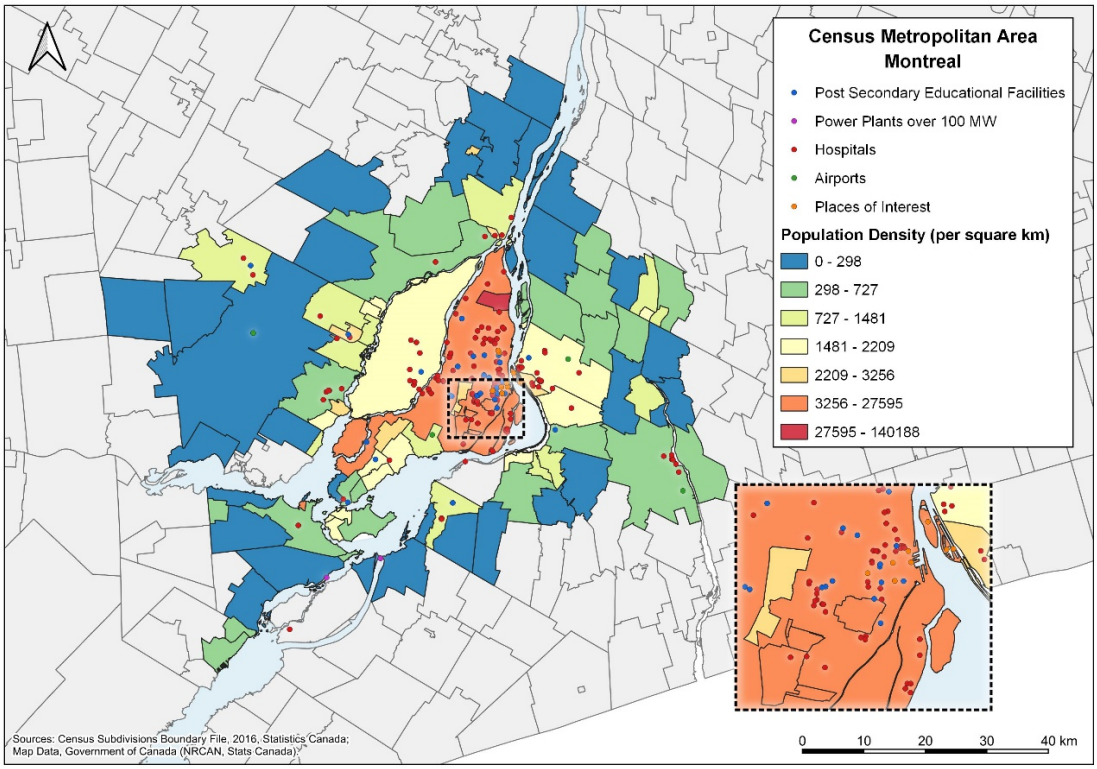

Figure 3: A map of Montreal detailing population density and points of interest.
Source: Authors

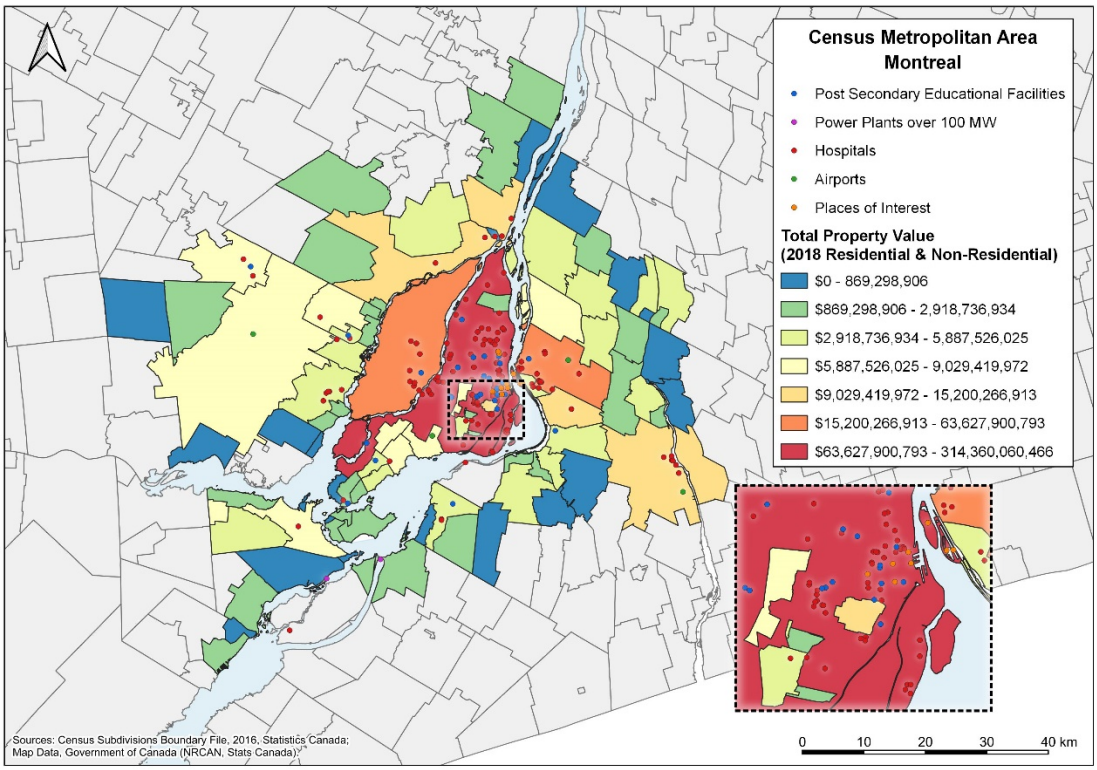

Figure 4: A map of Montreal detailing property value and points of interest.
Source: Authors

Naturally, the downtown core is the most densely populated area. Importantly, this is also the area where property values are highest. Consequently, striking Montreal's downtown core offers a belligerent the advantages of having sewn fear and achieving immediate economic damage. Again, the downtown core is rife with medical facilities, post-secondary education facilities, and other points of interest. Belligerents seeking to cause objectives of policy change on the international level, influencing public attitudes, or discrediting a government seemingly unable to protect its own citizens might choose to target these sites. Somewhat more obscure in the inset are critical elements of national infrastructure, including rail and road bridges. A strike here would also impact operations in the St. Lawrence Seaway—an essential trade route. More specific information and direct impacts of successful missile strikes on select locations are detailed in Table 2.

Conclusions

A review of the GTD and public media illustrates that Canada is not immune to attacks perpetrated by non-state actors. These attacks are typically of small scale involving explosives or small arms. Globally, missiles have also been used in attacks by non-state actors. More advanced missile systems are continuously in development by state actors, including North Korea, Russia, and China. Recent tests have illustrated success at developing hypersonic weapons designed to evade interception by missile defence systems.[21] Whether perpetrated by a state or non-state actor, there are ample opportunities for belligerent actors to pursue a variety of objectives by striking targets in Canada, including the provocation of state-on-state warfare. Mapping software such as ArcGIS can be used to identify regions of the country where these potential targets are concentrated, thereby increasing the impact of a successful strike.

Targets	**Details**	**Potential Impacts**
Canadian Forces base (CFB) Bagotville	Two CF-18 Tactical Fighter Squadrons Combat Support Squadron Radar Squadron	• Tactical air power neutralized in Eastern Canada • Reduction in search-and-rescue capability in the region • Static radar capability reduced, quick deployment capability neutralized
CFB Halifax	Seven Halifax-class frigates Six Maritime Coastal Defence Vessels Two Victoria-class submarines Sea Training Facilities Fleet Maintenance Facility	• Maritime power vastly reduced in the Atlantic, with the exception being any vessels deployed or otherwise at sea • Domestic support capability for maintenance of naval assets on the East Coast neutralized • Force generation of naval crews supporting the Atlantic fleet neutralized; increased pressure on Naval Training Development Centre (Pacific)
Montreal	Suncor Refinery	• Reduction of up to 137,000 barrels per day in the supply of refined petroleum products in Eastern Canada • Destruction of stored capacity of 1.4 billion litres of crude oil
	Énergir Natural Gas Line	• Service of natural gas to 205,000 customers

		disrupted
	Port of Montreal	• Canada's second largest port and largest accessible through the Atlantic • Monthly imports of 0.6 million metric tonnes of cargo and 1.45 million metric tonnes of bulk goods disrupted • Monthly exports of 0.5 million metric tonnes of cargo and 1.2 million metric tonnes of bulk goods disrupted • Major impact on the importation of crude and export of refined products • Major imported goods through the port of Montreal include iron ore, grains, sugar, fertilizers, and salt • Montreal handles twenty times the number of standard-sized sea containers than the combination of alternative ports: Port of Halifax, St. John, and Port de Québec
Montreal	St. Lawrence Seaway	• The seaway serves over 200 million tonnes of cargo annually, supports 329,000 jobs, and generates $59 billion in economic activity between Canada and the US[22] • The St. Lambert and Ste. Catherine Locks (14 nautical miles from the Port of Montreal) are 80 feet wide[23] • Destroying this lock would sever the seaway from the Montreal port it is designed to serve
	Victoria Bridge (Route 112)	• Two lanes; two rail tracks (CNR's main line) • Next closest rail crossing over the St. Lawrence Seaway is Quebec City • Destroying Victoria Bridge forces rail freight departing the Port of Montreal en route to New England to be redirected through the CSX DeWitt railyard in Syracuse, NY
	Pont Samuel de Champlain (Hwy 10)	• Eight lanes • Serves 50 million road crossings, annually[24] • Equivalently, a reduction of 40 per cent of the transit capacity across the St. Lawrence River at Montreal
	Pont-tunnel Louis-Hippolyte Lafontaine (Hwy 20 – Trans Canada)	• Six lanes • Serves 44 million road crossings annually[25] • Equivalently, a reduction of 35 per cent of the transit capacity across the St. Lawrence River at Montreal
	Pont Jacques-Cartier	• Five lanes

		• 30.5 million crossings annually[26] • Equivalently, a reduction of 25 per cent of the transit capacity across the St. Lawrence River in Montreal
	Pierre Elliot Trudeau Airport	• The fourth busiest airport in Canada • Serving 5.2 million passengers annually • Approximately 100,000 aircraft movements in 2021[27] • One of four national Air Canada hubs
	Montreal General Hospital	• Level I trauma centre (one of three in Quebec) • 479 beds
	McGill University Health Centre	• Eight research programs, including 500 active members and approximately 1,500 research trainees • Generation of over 2,500 peer-reviewed scientific publications • Approximately 25,000 surgeries annually[28]
	University of Montreal Health Centre	• 1,259 beds • Among the largest hospitals in North America • Level II trauma centre
	Jewish General Hospital	• 637-bed teaching hospital.[29]
	Hôpital du Sacré-Coeur de Montréal	• 554 beds • One of three Level I trauma centers in the province
	McGill University	• Approximately 40,000 students across thirteen faculties, 11 per cent of which are Ph.D. students[30]
	Concordia University	• Approximately 50,000 students across four faculties[31]
	L'Université du Québec à Montréal	• Approximately 37,000 students across six faculties[32]
	Université de Montréal	• Approximately 65,000 students across fifteen faculties[33]

Table 2: Potential Targets in Eastern Canada and Impacts.
Source: Authors

About the Authors

Dr. **Geoff Pond** is an Associate Professor in the Department of Management at the Royal Military College, where he teaches the MBA, Applied Military Science, and undergraduate business programs. Dr. Pond is a licensed engineer through Professional Engineers Ontario. His research focuses on engineering and logistics management.

Emilie Breuvart holds a Bachelor's degree in Geography awarded by Queen's University and works as part of the Royal Military College Green Team, where she contributes GIS analysis in support of a variety of projects.

Dr. **Andrew B. Godefroy** is an associate professor (adjunct) at the Royal Military College of Canada, where he specializes in missile and space research. He served as an engineering officer in the Canadian Armed Forces for thirty-two years, including time as both a senior Canada-US space policy analyst as well as a space operations officer. An authority on international space programs, Andrew is the author of two books and several scholarly articles on ballistic missiles and space research and development.

Cindy Lin is a graduate of the Smith School of Business at Queen's University and is currently pursuing her J.D. at the University of Toronto Faculty of Law. Her previous work includes leading the digital marketing strategy at the Conflict Analytics Lab, a research consortium applying artificial intelligence and data analytics to case law in order to democratize access to justice. She also interned in the US M&A Tax group at KPMG Canada. At law school, she is an Associate Editor for the University of Toronto Faculty of Law Review and an executive member of the Business Law Society.

Endnotes

[1] Andrew B. Godefroy, "Transformation and the Army of Tomorrow," in *Toward Land Operations 2021: Studies in Support of the Army of Tomorrow Force Employment Concept*, eds. Andrew B. Godefroy and Peter Gizewski (Ottawa, Canada: Department of National Defence 2009), https://publications.gc.ca/collections/collection_2011/dn-nd/D2-188-1-2009-eng.pdf.

[2] U.S. Congress, House Armed Services Committee on Strategic Forces (March 1, 2022) (statement of Charles A. Richard, Commander, United States Strategic Command) https://www.congress.gov/117/meeting/house/114435/witnesses/HHRG-117-AS29-Bio-RichardC-20220301.pdf.

[3] "North Korea Tests Banned Intercontinental Missile," *BBC News*, March 24, 2022. https://www.bbc.com/news/world-asia-60858999.

[4] U.S. Library of Congress, Congressional Research Service (CRS), *Hypersonic Weapons: Background and Issues for Congress* by Kelley M. Sayler, R45811 (February 13, 2023), https://crsreports.congress.gov/product/pdf/R/R45811/35.

[5] Dogucan Mazicioglu and Jason R.W. Merrick, "Behavioral Modeling of Adversaries with Multiple Objectives in Counterterrorism" *Risk Analysis* 38, no. 5 (2018): 962-977, https://doi.org/10.1111/risa.12898; Ralph L. Keeney, "Modeling Values for Anti-Terrorism Analysis," *Risk Analysis* 27, no. 3 (2007): 585-596, https://doi.org/10.1111/j.1539-6924.2007.00910.x.

[6] Sarah V. Marsden, "Successful Terrorism: Framework and Review," *Behavioral Sciences of Terrorism and Political Aggression* 4, no. 2 (2012): 134–150, https://doi.org/10.1080/19434472.2011.582705.

[7] See "Global Terrorism Database," The National Consortium for the Study of Terrorism and Responses to Terrorism (START), last accessed August 25, 2022, https://www.start.umd.edu/gtd.

[8] START, *Global terrorism database codebook: Methodology, inclusion criteria, and variables* (College Park, MD: University of Maryland, August 2021), https://www.start.umd.edu/gtd/downloads/Codebook.pdf.

[9] START, "Global Terrorism Database."

[10] Robert D. McFadden, "Iran Rebels Hit Missions in 10 Nations," *The New York Times*, April 6, 1992, https://www.nytimes.com/1992/04/06/world/iran-rebels-hit-missions-in-10-nations.html; "Deadly embassy attack in Ottawa," *CBC Archives*, https://cbc.ca/player/play/1403698588.

[11] START, "Global Terrorism Database."

[12] See Article 22, "Vienna Convention on Diplomatic Relations and Optional Protocol on Disputes," signed April 18, 1961, *United Nations Treaty Series*, vol. 500, no. 7, https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf. Canada ratified the treaty in 1966; see Canada Department of External Affairs, *Diplomatic relations: Vienna convention* (Ottawa: Queen's Printer, 1970), https://publications.gc.ca/collections/collection_2016/amc-gac/E3-1966-29.pdf.

[13] "Alleged 'al-Qaeda-supported' plot against Via train thwarted," *CBC News*, April 22, 2013, https://www.cbc.ca/news/politics/alleged-al-qaeda-supported-plot-against-via-train-thwarted-1.1377031.

[14] Isabel Teotonio, "Toronto targets picked, terror trial told," *Toronto Star*, June 10, 2008, https://www.thestar.com/news/gta/2008/06/10/toronto_targets_picked_terror_trial_told.html.

[15] The detail in this table is drawn from Table 2 in Paul Chouinard and Doug Hales, *The National Critical Infrastructure Interdependency Model – Volume IX: Characterizing the Transportation Sector*, DRDC-RDDC-2020-D099 (Ottawa, Canada: Defence Research and Development Canada, September 2020), 7-8, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc350/p812531_A1b.pdf.

[16] START, "Global Terrorism Database."

[17] START, "Global Terrorism Database."

[18] START, "Global Terrorism Database."

[19] Marsden, "Successful Terrorism," 134–150.

[20] "2016 Census – Boundary Files," Statistics Canada, last modified November 13, 2019, https://www12.statcan.gc.ca/census-recensement/2011/geo/bound-limit/bound-limit-2016-eng.cfm; "Download, Census Profile, 2016 Census," Statistics Canada, last modified August 25, 2017, https://www12.statcan.gc.ca/census-recensement/2016/dp-pd/prof/details/download-telecharger/comp/page_dl-tc.cfm?Lang=E; Joanne Hans, email message to Geoff Pond, September 9, 2022; "The Open Database of Educational Facilities (ODEF) Metadata document: concepts, methodology and data quality," Statistics Canada, last modified November 28, 2022, https://www.statcan.gc.ca/en/lode/databases/odef/metadata; "The Open Database of Healthcare Facilities (ODHF) Metadata document: concepts, methodology and data quality," last modified October 19, 2022, https://www.statcan.gc.ca/en/lode/databases/odhf/metadata; "Airports - Canadian Airports with Air Navigation Services," May 19, 2021, https://open.canada.ca/data/en/dataset/3a1eb6ef-6054-4f9d-b1f6-c30322cd7abf/resource/d805cd5e-b91c-4598-849f-ca2d89f72ed9#additional-info; "Energy infrastructure and resource potential of North America," Natural Resources Canada, last modified March 10, 2017, https://geoappext.nrcan.gc.ca/GeoCanViz/map/nacei-cnaie/en/index.html.

[21] CRS, *Hypersonic Weapons*, 17.

[22] "Ship Transits Seaway's St. Lambert Lock Bringing Vital Goods to Market," The St. Lawrence Seaway Management Corporation, April 1, 2020, https://greatlakes-seaway.com/en/news/ship-transits-seaways-st-lambert-lock/.

[23] "Locks, Canals & Channels," The St. Lawrence Seaway Management Corporation, last accessed May 31, 2023, https://greatlakes-seaway.com/en/the-seaway/our-locks-and-channels/.

[24] "Presentation," Samuel de Champlain Bridge, last accessed May 31, 2023, https://www.samueldechamplainbridge.ca/about-us/presentation/.

[25] René Bruemmer, "Rebuilding Louis-Hippolyte-la-Fontaine Tunnel a four-year ordeal," *Montreal Gazette*, June 21, 2018, https://montrealgazette.com/news/local-news/rebuilding-louis-hippolyte-la-fontaine-tunnel-a-four-year-ordeal.

[26] "About," The Jacques Cartier and Champlain Bridges Incorporated, last accessed May 31, 2023, https://jacquescartierchamplain.ca/en/structures/jacques-cartier-bridge/about/.

[27] See "Aircraft Movements" in "Passenger traffic and aircraft movements," Aéroports de Montréal, last accessed May 31, 2023, 5, https://www.admtl.com/sites/default/files/2022/ADM_Statsdet_2022_EN.pdf.

[28] *Rapport annuel de gestion 2020/21* (McGill University Health Centre, 2021), https://muhc.ca/sites/default/files/docs/annual-reports/MUHC_Annual-Report_2021_FINAL_WEB.pdf.

[29] "Our Hospital," Jewish General Hospital, last accessed May 31 2023, https://www.jgh.ca/about-us/our-hospital/.

[30] "Quick *facts*," McGill University, last accessed May 31, 2023, https://www.mcgill.ca/about/quickfacts.

[31] "Concordia University," I choose Montréal, last accessed May 31, 2023, https://www.jechoisismontreal.com/en/montreal-educational-institutions/concordia-university/#:~:text=Concordia%20is%20among%20the%20largest,ratio%20of%2027%20to%20one.

[32] "UQAM in numbers," Université du Québec à Montréal, last accessed May 31, 2023, https://uqam.ca/en/information/numbers/.

[33] "Université de Montréal," I choose Montréal, last accessed May 31, 2023, https://www.jechoisismontreal.com/en/montreal-educational-institutions/universite-de-montreal/.

CAJ
The Canadian Army Journal

NATO ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE POUR L'OTAN