Connecting the dots on Canada’s connected battlespace

Kevin Budning
Norman Paterson School of International Affairs, Carleton University, Canada

Alex Wilner
Norman Paterson School of International Affairs, Carleton University, Canada

Guillaume Cote
Collins Aerospace, Canada

Abstract
A “connected battlespace” (CB) aims to leverage emerging technologies, such as low Earth orbit satellites, internet of things devices, cloud computing, and artificial intelligence, in order to collect, process, and disseminate large quantities of data in real time, thereby providing decision-makers with the ability to respond to threats faster and with more precision. Despite its promise, as a concept, a CB is still misunderstood, underdeveloped, and understudied. In an effort to fill this gap, this policy brief describes several key findings derived from an expert stakeholder workshop that the authors convened in July 2020. Workshop participants probed several questions about the development of Canada’s CB infrastructure, touching on a number of themes, including alliance partnerships, emerging technology, procurement, national security, and defence strategy. Our article synthesizes and analyzes key discussions held during this workshop.

Corresponding author:
Alex Wilner, Norman Paterson School of International Affairs, Carleton University, Richcraft Hall, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.
Email: alex.wilner@carleton.ca
As an emerging concept, a “connected battlespace” (CB) aims to enable seamless, real-time network connectivity between various military assets across all domains of contemporary warfare. Its goal is to leverage technological innovations in low Earth orbit satellites, internet of things devices, cloud computing, and artificial intelligence (AI), both to provide defence planners with greater awareness, control, coordination, and precision and to enable any sensor to inform any shooter in any domain. Despite the benefits that stem from achieving a CB, the concept is still in its infancy, generally misunderstood, underdeveloped, and understudied. This policy brief aims to fill this gap by investigating the benefits, barriers, and opportunities associated with the Canadian Armed Forces’ embrace of the concept. We argue that properly developing a CB will require broad cooperation within Canada’s security partnerships—notably, the North American Aerospace Defence Command (NORAD) and the Five Eyes—and between the Department of National Defence and domestic industry players. Our findings largely derive from an expert stakeholder workshop convened in July 2020 as part of a multiyear Mitacs grant. Attended by over seventy-five leading military specialists, academics, and policy experts, the workshop probed several practical questions about the development of Canada’s CB infrastructure, exploring the nexus between imagining a CB and actually building one. The article unfolds in three sections, beginning with a brief description of the CB concept with highlights from Canadian allies, turning next to assessing core findings derived from the workshop, and concluding with a discussion of next steps for research and policy. The underlying theme is that Canada can and should do more.

**CB: A primer**

Military services are traditionally divided across six domains, including air, land, maritime, space, information, and cyber, with the last three functioning as the connecting link uniting them all. Until recently, forces active in each domain operated almost exclusively via siloed information sharing platforms, a stovepipe approach to command and control (C2) that hindered interoperability between and among various military assets. A CB addresses this deficiency by linking the various network-capable devices and sensors from the Air Force, Army, Navy, Special Operations Forces, and space-based forces into a single aggregate network,

---

1. Connected battlespace is often referred to as Joint All Domain Command and Control (JADC2). We use these terms interchangeably throughout this paper.

2. The project, “The Impact of Emerging Technologies on Defence Policy,” is jointly managed by Dr. Wilner and Dr. Cote. The project received a 2020 Mitacs Accelerate grant (IT17023).
enabling commanders to “rapidly understand the battlespace, direct forces faster . . . and deliver synchronized combat effects across all domains.” A by-product of the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) framework, a CB relies primarily on data-driven technologies to establish a common defense network, programmed to capture, process, transmit, and interpret information in real time in support of pan-domain operations. A CB, then, is just as much about building connectivity and information bridges between geographically dispersed assets, platforms, and personnel, as it is about doing so across all traditional and emerging domains of warfare.

In the US, the drive for reaching a CB is being pursued by different branches of the military. For instance, the US Air Force’s Advanced Battlespace Management System (ABMS) recently tested an experiment in which a SpaceX Starlink constellation was connected to an AC-130 gunship. As a second illustration, the US Army’s Tactical Intelligence Targeting Access Node is developing a system that leverages “space and high altitude, aerial, and terrestrial layer sensors to provide targetable data to fires networks.” Given the intense information requirements of these and other programs, on-demand data storage and processing have become paramount. In response, the US Department of Defense recently awarded the US Joint Enterprise Defense Infrastructure (JEDI) a contract to create a single-service cloud storage platform that hosts and distributes data to US military assets around the world. The UK and Australia are likewise exploring ways to develop their own CBs. The UK’s former Niteworks program, which addressed a range of complex questions through its extensive partnership with private firms and academic institutions, played an instrumental role in the development of Morpheus, the first installation of the UK’s defence-as-a-platform infrastructure that is meant to ensure that its Ministry of Defence can select and deploy new capabilities more quickly and efficiently. And Australia’s Science, Technology, and Research Shots program also seeks to modernize the military by partnering defence officials with those in academia and industry. These programs have helped develop new procurement processes, knowledge-sharing arrangements, and innovative technology that serve as the foundation for a CB. From an allied perspective, building this capacity is critical. Unlike industrial-age interoperability that focused

3. Joint All Domain Command and Control (JADC2) (Washington DC: CRS In Focus, IF11493, Version 10, 16 November, 2020), https://fas.org/sgp/crs/natsec/IF11493.pdf (accessed 1 February 2021).
4. Valerie Insinna, “Is the Air Force’s Advanced Battle Management System program gearing up to be the next major acquisition failure?” C4ISRNET, April 2020, https://www.c4isrnet.com/ (accessed 8 October 2020).
5. Sean Kimmons, “TITAN system being developed to tie ‘deep sensing’ to long-range fires,” Army News Service, 24 October 2019, https://www.army.mil/article/228867/ (accessed 8 October 2020).
6. Heather Kuldell and Frank Konkel, “A look at key moments in one of the Pentagon’s most important tech procurements,” Next Gov, https://www.nextgov.com/feature/jedi-contract/ (accessed 1 February 2021).
7. “The value of partnership,” Inform: An Update on Defence Decision Makers Info, no. 5 (February 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692471/niteworks-inform-issue-5-march2018.pdf (accessed 8 October 2020).
(simply, though not simple) on integrating allied platforms, information-age interoperability entails “sharing large amounts of data, machine-to-machine, over networks to link sensors, platforms, and [C2] nodes” together, a far more complicated, costly, and complex task.\(^8\) As a consequence of political challenges, bureaucratic inertia, and a slow-moving procurement system, Canada has yet to introduce any initiative of comparable scope, scale, funding, or ambition to the US, UK, or Australian programs.

**Canada’s CB: Workshop findings\(^9\)**

The future landscape of a CB in Canada remains uncertain. What Department of National Defence mechanisms allow for an effective integration of new technology with legacy systems? How can the Department of National Defence achieve a coherent program that allows for a compatible integration of C4ISR and emerging data-driven technologies across Canada’s current and future military platforms? And how will a CB—or a failure to establish one—influence Canada’s relationships with its allies? What follows is a discussion of these and other questions derived from our stakeholder meeting.

**The use and utility of a Canadian CB**

Does Canada need a CB? From a strategic perspective, geopolitical considerations and developments suggest that it does. A CB will help Canada prepare for a new generation of threats and operations stemming from the return of great power (and data-driven) competition between the US, China, and Russia. Investing in and developing the technologies that advance a CB would signal to Canada’s alliance partners (and adversaries) that it takes interoperability and its defence commitments seriously. Canada should assume that developing a CB is an inevitable process, not an optional one. As stakeholders reiterated, a CB will help states to achieve precise decision-making that includes “a synchronization of effects” across the domains of warfare.\(^10\) This synchronization will enhance military capability, help deter adversaries, and improve freedom of action. The opposite risk, then, also holds: without a CB, Canada hinders its ability to integrate and calibrate new

---

8. Matt Isler, “Data is the foundation of JADC2, and we need allies and partners ‘built in,’” Medium, 16 April 2020, https://medium.com/@matt_53137/data-is-the-foundation-of-jadc2-and-we-need-allies-and-partners-built-in-c31247099ee9 (accessed 8 October 2020).

9. During our workshop, which was held via Zoom, participants were divided into three breakout rooms—Defence and Strategic Planning, NORAD Modernization, and Five Eyes—contingent on their preference and level of expertise. A series of related discussion questions were circulated among participants beforehand, which helped shape the discussion. A subsequent summary report was written and disseminated among participants (“The Making of Canadian Connected Battlespaces: Virtual Workshop Report,” August 2020). In keeping with Chatham House Rule, participants’ identity, title, rank, and remarks were neither recorded nor disclosed.

10. This reference, and other subsequent ones, stem from the July 2020 stakeholder workshop, and to our subsequent report, “The Making of Canadian Connected Battlespaces: Virtual Workshop Report” (August 2020).
and legacy systems with those of its allies, potentially fracturing its relationships and degrading trust within major coalitions and losing its ability to provide meaningful input on allied decision-making. And when—rather than if—the US CB emerges, Canada may jeopardize some of its sovereign control, in the event, for instance, that the US dictates a way forward regarding NORAD and comes to expect Canadian compliance. By bridging and blending all domains, some stakeholders warned that a US CB will render NORAD’s narrow focus on air defence effectively obsolete. On this, Canada and the US have yet to express a mutual understanding of what projects, technologies, and initiatives are needed for joint investment. Despite Canada’s promising moves on Arctic security, specifically with the North Warning System and satellite development, its greater position within NORAD (especially under a CB) remains ambiguous. Indeed, as stakeholders noted, NORAD modernization is not fully addressed in “Strong, Secure, Engaged.” Canada has yet to table a coherent national strategy and framework on the subject, leading some stakeholders to conclude that the US will eventually move forward regardless.

**Political leadership is necessary but not sufficient**

Assuming Canada comes to accept that a CB is a necessity, what needs to happen next? Four things must align: intention; programming; resources; and knowhow. Intention will involve the eventual release of a high-level political declaration mandating organizational units that make joint-force development a strategic priority. In this regard, Canada has expressed interest, yet it has not exuded the same degree of commitment as its American and Five Eyes counterparts. Second, achieving a CB will depend on consistent and authoritative programming from military leaders, made possible by explicit assent. Such programming should promote not only top-down control but also bottom-up innovation by technicians and engineers. In these programs, military leaders will need to integrate mechanisms for cooperation with industry players, such as vehicles for procurement innovation and joint experimentation. Third, leveraging resources involves authorizing procurement agents to spend on targeted programs and deliverables with increased flexibility. The need for innovative procurement processes is crucial because, as stakeholders stressed, the slow pace and conservatism of current military procurement is the greatest impediment to Canada’s ability to introduce the technology, talent, and organizational capabilities needed to build a CB.

Finally, for knowhow, Canada will need to find creative ways to work more closely with industry partners in developing a CB. To a certain degree, the Department of National Defence and the Canadian Armed Forces currently lack the proper systems, personnel, and technical abilities needed to support the successful introduction of a CB. Moreover, in a context where data-driven technologies are evolving faster than requirements are identified, industry should be viewed as a strategic partner that can introduce new technology and identify innovative processes. Working with industry is Canada’s best shot at answering some of the most elusive questions regarding data—most notably, how to acquire data.
at scale, how data can be used to augment decision-making, how to harden information stores from adversaries, and how to engineer what amounts to a self-reinforcing defence data ecosystem. Expanding the relationship between the Department of National Defence, the Canadian Armed Forces, Defence Research and Development Canada, and industry and academia sounds like a cliché, but doing so is also imperative for the formation of a CB. Well-established defence businesses are equipped to drive alignment on complex multi-stakeholder project portfolios, test and develop new technologies, and work with partners in establishing and absorbing best practices.

**Canada needs to rethink data**

If Canada succeeds in bridging intention, programming, resources, and knowhow together, what role do data play? Two shifts in perspective will be needed. First, stakeholders suggested that the Canadian government will need to adopt a degree of comfort with “fail-fast” models of technological experimentation. Some pieces of a CB are still being conceived of, let alone built; adapting to this technological uncertainty will help Canada manage the transition to and adoption of emerging technology. Second, from a CB perspective, data cannot be understood as existing solely in closed-off siloes. Rather, data should be understood as a common building bloc, as the raw materials that are foundational to an enterprise data platform. In connecting the country’s military infrastructure, an incremental approach to data would be most pragmatic and cost-effective. Given the difference in size and scale with the US, Canada does not need to replicate emerging American programs, like ABMS or JEDI, in order to make meaningful progress towards a CB (though some stakeholders did suggest that JEDI provides a good example of the type of collaboration between academia, government, military, and the private sector Canada could follow). Multiple, simultaneous, and smaller integrations can take place that build on existing structures, meeting Canada’s financial and capacity constraints. In other words, data integration could be accomplished on a piece-by-piece basis. Furthermore, the Department of National Defence and the Canadian Armed Forces need not yet purchase new equipment that enables connectivity for building a CB. Many existing platforms and technologies that currently exist can be used as a baseline to begin planning for and testing new data, software, and network integrations. This is about getting disparate pieces of equipment “talking to” one another in a novel and nuanced way.

**Leveraging Canada’s comparative advantage**

With a Canadian CB in place, what additional windfall might Canada come to expect? As more countries seek to create pan-domain connectivity, Canada will be positioned to leverage its comparative technological advantage, becoming not a consumer but rather a global contributor and leader of allied military innovation. And, as stakeholders noted, Canada would subsequently benefit by shaping related standards and processes, further cementing its advantage. Canada has already
invested heavily in satellite research and development and has expertise in the areas of space-based sensing, underwater domain awareness, wide-band high-frequency communications, beyond the horizon radar, and software-defined radios, all of which will come into play in a CB. Stakeholders suggested that Canada could seize the opportunity to identify these, along with other niche technologies, that it could invest in and build domestically. Capitalizing on this intellectual property, standardization, and other innovations through export to and further development with allied states will prove economically important.

**Next steps for research and policy**

In February 2020, when asked about the defence priorities of the US, General John Hyten, vice chairman of the US Joint Chiefs of Staff declared that a CB is “the biggest key to the future.” Whoever is first to develop such a system, he argued, will “have a significant advantage over everybody in the world for a long time, because it’s the ability to integrate and effectively command and control all domains in a conflict or in a crisis.” Indeed, from a strategic and operational point of view, a CB is a game changer. And, yet, from a Canadian perspective, more research is needed in three distinct areas.

First, as we acknowledge, building a CB is an ambitious project that is still uncertain. Many technological and scientific questions persist and need to be explored in greater technical detail if a CB is to prove viable: How will the thousands upon thousands of cross-domain sensors, and new and legacy systems, actually link up and communicate with each other? Who will control and manage the flow and storage of data—a government body, a public–private consortium, or some other actor altogether? Will the cloud remain secure, and what are the risks if it does not? What are the ramifications of erratic AI systems? Will decision-makers and military leaders trust them? And what hardware and software solutions still need to be discovered and developed? Clearly, more scientific, technical, and laboratory research is still needed, but a failure to imagine future possibilities should not get in the way.

Second, it is possible, contrary to one of our central arguments, that Canada could gain by waiting and observing how the US and other allies fare with their own CB investments and developments. Indeed, some stakeholders suggested that the US was moving too quickly with its procurement of emerging technology, acquiring new tools faster than they could plan for their effective use. By lagging behind, Canada gains a degree of efficiency—learning from the American experience and adopting its approach if and when the US succeeds, ultimately becoming

---

11. Shaun Haney, “Low-earth satellites getting closer to delivering high speed rural Internet,” *RealAgriculture*, 25 September 2020, https://www.realagriculture.com/2020/09/low-earth-satellites-getting-closer-to-delivering-high-speed-rural-internet/ (accessed 8 October 2020).

12. Colin Clark, “Gen. Hyten on the New American Way of War: All-Domain Operations,” *Breaking Defense*, 18 February 2020, https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/ (accessed 8 October 2020).
more, rather than less, interoperable with the US military over time. More research is needed on theoretically untangling the conceptual relationship between strategic patience and strategic gain within an allied setting. Empirical studies should likewise explore lessons from Canada’s and other countries’ past experience with this phenomenon. And policy research should explore the associated political effects of Washington’s perception of Canada’s free-riding strategy, especially in an era of increased protectionism and isolationism.

Third, more discussion and debate surrounding the policy trade-offs and implications of pursuing a CB are needed in Canada. On geopolitical, defence, and security terms, we argue that investing in the technology is both a prudent and worthwhile endeavour. But investments in defence usually come at the expense of other Canadian initiatives; some compromise will be required. As one stakeholder noted, defence does not usually rank very highly on the list of voter priorities. To a certain degree, the eventual investment needed to build a CB will focus Canada’s attention on international rather than domestic considerations, and on North American rather than local and regional concerns. However, without tangible action and explicit consent by key decision-makers, Canada’s timeline for advancing this program remains uncertain. Until then, researchers and defence planners must weigh the trade-offs, parse through the ambiguities, and work together in connecting the dots on Canada’s CB.

Acknowledgements
The authors express their sincere gratitude to Sean Murphy and Hannah Diegel for their tireless efforts in organizing the stakeholder workshop and assisting in researching and reviewing this article.

Declaration of Conflicting Interests
The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by Mitacs, Grant Number: IT17023.

ORCID iD
Alex Wilner https://orcid.org/0000-0003-2087-252X
Author Biographies

Kevin Budning is a PhD candidate at the Norman Paterson School of International Affairs, Carleton University, Ottawa, Ontario, Canada.

Alex Wilner is an Associate Professor of International Affairs at the Norman Paterson School of International Affairs, Carleton University, Ottawa, Ontario, Canada.

Guillaume Cote is the Principal Strategy Manager at Collins Aerospace, Ottawa, Ontario, Canada.