Policy

Brief

July 2020

Author

Kristen Csenkey

The (Cyber) Future of Procurement

Defence & Security Foresight Group

About the Author

Kristen Csenkey is a PhD Candidate in Global Governance at the Balsillie School of International Affairs through Wilfrid Laurier University (WLU). Her research is on the politics and policy of cyber governance, security, and hybrid threats. Kristen graduated from the University of Toronto, holds an MA in anthropology, and completed her Master of Applied Politics degree from WLU.

Funding Acknowledgment

This Working Paper was funded by the Defence and Security Foresight Group which receives funding from the Mobilizing Insights in Defence and Security (MINDS) program designed to facilitate collaboration and mobilize knowledge between the Department of National Defence, the Canadian Armed Forces, and academia and other experts on defence and security issues. Through its Targeted Engagement Grants, collaborative networks, scholarships, and expert briefings, MINDS works and collaborates with key partners to strengthen the foundation of evidence-based defence policy making. These partnerships drive innovation by encouraging new analyses of emerging global events, opportunities, and crises, while supporting a stronger defence and security dialogue with Canadians.

The development of this policy brief was inspired by the working paper "Cyber Futures: A Preliminary Scanning and Foresight Report" written by Dr. Alex Wilner.

For more information on our network please visit our website uwaterloo.ca/dsf-group or email us at dsfgroup@uwaterloo.ca

Introduction

An investment in cyber is essential to advance Canadian defence capabilities. The Department of National Defence (DND)/Canadian Armed Forces (CAF) needs to invest in an update to its current procurement frameworks to reflect the dynamic futures of the cyber domain. This means using a strategic foresight approach to procurement to effectively engage in conflict situations both now and in the future.

Problem: Constant Catchups and Unkowns

Procurement is an endless game of catchup. It involves acquiring resources and technologies to fulfill program needs. At times, this is a slow process that is constrained by budgets and changing priorities and is guided by current and anticipated needs.

Effective long-term procurement planning can be difficult when: 1) future threats and 2) the tools and skills to address these threats are largely unknown. Threats develop quickly within modern conflict and the technologies to address them change at a faster pace than in the past. This is especially apparent within cyber warfare and hybrid conflict situations where technological development outpaces procurement cycles.

Short-term acquisition strategies are used to fill current gaps. This is meant to address immediate threats. Previous approaches to achieving operational effectiveness have not reflected the dynamisms of cyber warfare or breadth of possible future conflicts. This poses long-term planning challenges to anticipating threats, planning operations, and identifying the tools needed to deal with future threats.

Contextualizing Procurement and Canadian Defence

As per *Strong, Secure, Engaged: Canada's Defence Policy* (2017) (SSE), DND/CAF is tasked with reforming defence procurement to support military applications. SSE calls for the streamlining of the defence procurement process.

Cyber is frequently a separate area of procurement in DND/CAF. For example, the *Defence Acquisition Guide* (2016) (DAC) included separate, cyber-specific projects from other procurement project calls, such as automatic identification technology, electronic warfare support, and computer network operations.

The *Defence Capabilities Blueprint* (2018) (DCB) replaced the DAC and demonstrates an increased focus on cyber procurement projects. Cyber is identified as a Defence Capability Area (DCA) within the DCB and the Cyber Mission Assurance program is tasked with establishing cyber security requirements in the procurement process. It is meant to mitigate risks to operations in physical and cyber environments.

Recommendation: Incorporate a Strategic Foresight Approach to the Procurement Planning Process

Strategic foresight is a way to anticipate change and includes techniques such as environmental scans and scenario construction. It is not predictive, but seeks to show how emerging trends could impact the future. When this approach is applied to defence, it means recognizing that there are many possible futures of conflict, including how it is created, facilitated, and addressed.

DND/CAF can apply a strategic foresight approach to procurement in order to efficiently address future threats by:

1. Integrating cyber into all aspects of the procurement process. Future conflicts will undoubtably entail cyber aspects. Cyber is a separate domain of conflict and permeates all other domains[1]. Thus far, DND/CAF's procurement policy has separated cyber. Cyber considerations must be integrated into all procurement planning processes beyond ensuring interoperability of systems. DND/CAF needs to focus on agility to match the pace of technological change[2]. Although the DCA designations and the Cyber Mission Assurance program are steps in the right direction, they need to incorporate a strategic foresight dimension. New programs should focus on identifying future trends and tools instead of playing technological catchup.

2. Investing in the continuous development and promoting relevant skills-sets. Procurement entails more than purchasing the right equipment for future operations. It includes developing the skills needed to enhance operational capabilities and anticipate a variety of threats. Cyber technologies policies are important, but procurement must also go beyond physical hardware and equipment. It should include the knowledge and skill sets needed to achieve Canada's defence objectives. Future operations will need to have the capacity and capabilities to effectively execute their missions. The newly established Cyber Operator positions are a part of this 'knowledge procurement', but more investment is needed in attracting personnel with the relevant competencies for future cyber conflicts.

[1]Canadian Association of Defence and Security Industries (CADSI)."*The Cyber Collaborative Imperative: An Overview of Leading Government-Industry Collaboration Models and Practices in Cyber Defence*" 2020 Report https://www.defence-andsecurity.ca/UserFiles/Uploads/publications/reports/files/document-26.pdf

[2]Richardson, William, Kalen Bennett, Douglas Dempster, Philippe Dumas, Caroline Leprince, Kim Richard Nossal, David Perry, Elinor Sloan and J. Craig Stone. "Toward Agile Procurement for National Defence: Matching the Pace of Technological Change", CGAI Policy Paper. June 2020. https://www.cgai.ca/toward_agile_procurement_for_national_defence_matching_the_pace_of_technological_change