CADSI

PROCUREMENT AT CYBER SPEED

2021 Report | Canadian Association of Defence and Security Industries

TABLE OF CONTENTS

1.0 SUMMARY

From May 2019 to October 2020, CADSI interviewed 30 government, military, and industry cyber experts to identify military cyber procurement challenges and potential solutions.

CADSI's research concluded that government and industry agree on the core challenges impacting military cyber procurement:

1. The cyber procurement process is too slow and rigid to keep pace with cyber innovation and obsolescence cycles;
2. Most cyber procurement projects are too large and complex, introducing unnecessary risks for business and government;
3. Procurement professionals need new skills and training to keep pace with cyber innovations and to operationalize new procurement practices better aligned to cyber.

However, CADSI's research also concluded that government and industry are not aligned on how to solve these challenges. In part, this discord is attributable to a gap in Canada's cyber ecosystem – currently, there is no government-industry forum to discuss these issues and challenges or to collaborate on possible reforms, so little progress has been made.

Canada needs an institutionalized government-industry forum to discuss and obtain consensus around viable procurement reforms, and to support the implementation of solutions.

> CADSI believes that industry-government dialogue and collaboration are essential to resolving many of Canada's cyber challenges, including procurement, which further reinforces the key findings of our 2020 report, *The Cyber Collaboration Imperative*.[1]

The following government departments and organizations helped to shape this report: Department of National Defence (DND), Defence Research and Development Canada (DRDC), Canadian Centre for Cyber Security (CCCS), Communications Security Establishment (CSE), Global Affairs Canada (GAC), Innovation Science and Economic Development Canada (ISED), Public Safety Canada (PSC), Public Service and Procurement Canada (PSPC), Shared Service Canada (SSC), and Treasury Board Secretariat (TBS).

The following cyber-engaged firms helped to shape this report: ADGA, Calian, CCX Technologies, Clairvoyance Cyber Corp, CryptoMill Cybersecurity Solutions, FireEye, General Dynamics Missions Systems, IBM, KPMG, Microsoft, Rhea Group, root9B Canada, Sapper Labs, and the SecDev Group.

1 The Cyber Collaboration Imperative, CADSI, 2020.

2.0 COUNTERING THREATS COLLABORATIVELY

Canada and its closest allies are fighting a persistent cyberwar – a war born of the digital-era, borderless, impacting soldier and citizen alike. This cyberwar has spilled out across our networks and systems affecting public and private assets, democratic institutions, the military, security agencies, and Canadian citizens. The digital domain has been rendered unsafe for Canadians and dangerous for our women and men in uniform.

- In its *National Cyber Threat Assessment 2018*, CSE established that it is "now routinely blocking well over a billion malicious actions aimed every day at federal systems, databases and websites" and faces down "thousands of attempts to access and infiltrate government networks each day".[2]
- In its *2019 Update on Cyber Threats to Canada's Democratic Process*, CSE established that "half of all advanced democracies holding national elections have had their democratic process targeted by cyber threat activity;" a trend expected to increase.[3]
- DND networks, including those of DRDC and the Canadian Defence Academy (CDA), have been attacked and compromised on several occasions, going back to 2011.[4,5]

While Canada has been slow to adapt to the emerging cyber threat landscape, many of Canada's allies have built strong cyber defence capabilities to counter these threats. They have done so by recognizing the fundamental differences between traditional and cyber defence, and by harnessing the power of government-industry collaboration in their response:

1. In cyber defence, the role of the private sector is different and enhanced:
   - Industry drives a speed of innovation and attack that is faster than traditional defence;
   - Industry is responsible for more of the innovation, and plays a greater role in delivery of operations;
   - Industry owns and operates most of cyberspace, including the underlying networks and enabling technologies.
2. Cyber technologies present a unique risk profile and calculus that challenges current procurement approaches, and may result in a persistent techno-logical mismatch between Canada's military and its adversaries:
   - Given that adversaries can bring new capabilities online from scratch in 10 months or less, the perceived benefits of taking the time to thoroughly de-risk and compete procurements may be outweighed by the damage caused by an undefended attack;
   - Developing cyber solutions is best done through rapid iteration, and by breaking down larger problems into smaller, more discrete parts. This new paradigm does not mesh well with DND's current acquisitions approach.
3. No organization, operating in isolation, can keep pace with the rapid expansion of new cyber knowledge, technologies and practices:
   - Established government processes cannot meet or exceed cyber innovation cycles. Government needs to bring different expertise and knowledge together in new ways to develop and acquire cyber solutions effectively and on time;
   - The pace of cyber innovation places a premium on continuous reskilling, training, and knowledge exchange between government, industry, and academia.

Canada's current procurement system cannot account for cyber's aggressive obsolescence cycles, cross-platform integration challenges, or the unpredictable impacts of converging technologies. Shared Services Canada effectively summarized the digital-era procurement challenge when it noted that "we have shifted from discrete problems with fixed answers to holistic messes that require innovative approaches and collaborative solutions."[6]

2 National Cyber Threat Assessment, CSE, 2018.
3 Update on Cyber Threats to Canada's Democratic Process, CSE, 2019.
4 NATO Review: The History of Cyber Attacks – A Timeline, NATO, 2013.
5 Four Canadian Military Schools Affected by Cyberattack, Paul Waldie and Colin Freeze, Globe and Mail, 2020.
6 Agile Procurement for the Public Sector – A Primer, Emilio Franco, Shared Services Canada, 2017.

THE NATIONAL INTEREST: SOVEREIGN CAPABILITY

Canada is fortunate to have a world-class cyber industry. According to a 2020 ISED and Statistics Canada study, the sector comprises over 330 firms that build best-in-class technology sourced around the world. Canada's cyber industry generates over $1 billion in annual export revenues, and sells its products and services to all five-eyes allies.[1] Unfortunately, despite this strong domestic performance, the federal government continues to buy approximately 90% of its cyber technology from large foreign suppliers.[2] It is time for this situation to change. The best response to cyber threats is one that collaboratively mobilizes the innovation potential of domestic firms, especially SMEs.[3] There may be utility in better leveraging existing tools like the Industrial Technological Benefits (ITB) Policy and Value Propositions, already contained within the existing procurement framework, to help foster a stronger domestic industrial cyber base.

1 Statistical Overview of Canada's Cyber Security Industry in 2018, ISED, 2020.

2 From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence, CADSI, 2019. This report examined the publicly available government contracting data.

3 Army Modernization Strategy, U.S. Army, 2019; Small Business Strategy, Department of Defence, 2019; Small Businesses Behind Defence's Biggest Projects Recognized, Ministry of Defence, 2018.

3.0 THE IMPORTANCE OF PROCUREMENT TO SUSTAINED COLLABORATION

An effective procurement system for cyber goods and services is essential to a productive and collaborative relationship between government and industry.

> "We have to be able to buy the fruits of any collaborative labour at the end of the process. Without the ability to acquire the end solution, everyone's time is wasted, government and industry become frustrated, and the collaborative will evaporates."[7]

As cyber threats escalate and Canada rightfully intensifies investment in defensive cyber capabilities, an opportunity has been created. Canada's cyber resilience can be achieved through investment in sovereign capability. Leading domestic firms possess the capabilities and operational experience required to ensure Canada's digital defence. Now is the time for government and domestic cyber firms to work together to cultivate a broad domestic industrial base focused on cyber defence.

By emphasizing the procurement of domestic cyber capabilities and empowering large Canadian companies to maximize economic benefits harvested from the Canadian cyber industrial base, including through earlier application of the Value Proposition and Industrial Technological Benefits policies, enduring economic value can be created and sustained within this critical domestic industry.

Given that much cyber innovation takes place within industry, failing to improve cyber procurement risks placing significant limitations on one of the few channels through which industrial innovations can make their way into the hands of government operators.

This situation, left unresolved, has the potential to undermine Canada's national security by severely limiting the government's access to the most advanced, industry-driven cyber innovations and solutions critical to an effective defence against increasingly sophisticated and continuously innovating adversaries.

7 Quote from interview with government official.

4.0 CYBER PROCUREMENT SUCCESS FACTORS AND CHALLENGES

Interview respondents identified more than 20 government procurements and projects that demonstrated sub-optimal outcomes.

This research also revealed a set of characteristics that define successful cyber procurements:

- Operational and technical authorities are engaged early and remain committed;
- Projects deliver incremental results within 10-month cycles;
- Administrative and procedural overhead are consolidated and simplified;
- Communication between public and private stake-holders is direct and consistent;
- Core team member churn in the public sector is minimized over project lifetimes;
- Operational need is pre-validated, and re-validated periodically, by end-user clients;
- Industry is trusted with significant leeway to propose creative and out-domain solutions;
- The business-case and scope of work remain reasonable as the project adapts;
- One or more key public servants fully understands the systems at play and operational need;
- Strong executive support ensures that funding remains ready and available.

These success characteristics are likely applicable beyond military cyber procurements, especially given that some have been extracted from the successful cyber procurements of other Canadian federal departments and agencies.

However, anecdotal evidence collected through interviews suggests most military cyber procurements in Canada face moderate to significant challenges. Three consistent factors were identified as contributing to sub-optimal outcomes:

1. **The cyber procurement process is too slow and rigid to keep pace with cyber innovation and obsolescence cycles;**
2. **Most cyber procurement projects are too large and complex, introducing unnecessary risks for business and government;**
3. **Procurement professionals need new skills and training to keep pace with cyber innovations and to operationalize new procurement practices better aligned to cyber.**

5.0 PROBLEM 1: THE PROCUREMENT PROCESS IS TOO SLOW AND RIGID

Canada's federal government continues to apply industrial-era acquisition processes to digital-era challenges. Defence procurement continues to reflect a time when it was acceptable to acquire a weapons system or defensive platform over 10-20 years, given the system or platform would then operate effectively for 25 years or more.[8] These decades-long product lifetimes in traditional defence are a sharp contrast to obsolescence cycles in cyber that are measured in weeks and months.

A 2020 report by the Canadian Global Affairs Institute (CGAI) concisely summarized many of the core challenges impacting the defence procurement process, which are most acute in the Options Analysis and Implementation Stages.[9] While locking in requirements at the Options Analysis stage has proved a worthwhile strategy for traditional defence procurements, it can introduce risks and costs for faster moving cyber technologies, given how long the Options Analysis stage can take. The same problem arises at Implementation, where there is almost no ability to change project requirements, budget, or timeframe. This locks in solutions that risk becoming irrelevant and cost-ineffective.

The 2020 CGAI report also examined whether departmental financial constructs, as required by government-wide comptrollership practices, were implemented at DND in a manner that contributed to sub-optimal procurement outcomes. For example, the report noted how Vote 5 capital, used to buy new or improved capability at higher financial thresholds, triggers a long and complex procurement process that is not well suited to fast-paced technologies. Conversely, the report noted how Vote 1 capital, used to keep equipment up to date, triggers a more streamlined process better suited to fast-paced technologies, but is afforded a significantly lower financial threshold, and cannot acquire new or improved capability. The CGAI report suggested another Vote of capital may be required for advanced technologies like cyber, which better aligns their shorter product lifecycles with quicker, more flexible procurement rules and approaches, without sacrificing the appropriate financial thresholds required to field new and improved capabilities.

8 Toward Agile Procurement for National Defence: Matching the Pace of Technological Change, CGAI, 2020.

9 Options Analysis is when the business case is developed for all options and Implementation begins with the launch of a competition for desired services to select a supplier and then manage delivery.

6.0 PROBLEM 2: PROCUREMENT PROJECTS ARE TOO LARGE AND COMPLEX

Procurement strategies and related documentation in Canada need to be updated to reflect a more iterative approach to cyber procurement. This includes the need to strike a balance between smaller and steadier progressions of deliverables, managing overall system complexity, and ensuring consistent alignment of procured capabilities to operational intent.

Leading cyber procurement practices among Canadian allies favour new approaches, which break down complex projects into manageable subsets of tasks and challenges. By adopting these approaches, the level of technological sophistication and scale of solution can be gradually increased over time, which allows the customer (the Government of Canada) to review a measured progression of deliverables that moves steadily towards full-scale delivery of an operationally-relevant capability. This approach also offers the Government of Canada multiple off-ramps to replace non-performant technologies or suppliers, or to incorporate emerging innovations, which de-risks the procurement process, while making it more responsive to change.

> These types of iterative approaches have also been shown to secure greater levels of SME engagement – a priority in the U.S. and UK, where multiple reports have concluded that SMEs are key drivers of cyber and digital innovation.[10]

CHALLENGES AND BOTTLENECKS IN THE PROCUREMENT PROCESS

At a minimum, a project – a proposal to purchase a new capability for DND – must progress through 84 gates or approvals, grouped into Project Phases, before the project office can issue an RFP. DND's process is set out in the Project Approval Directive, which establishes five Standard Project Phases – Identification, Options Analysis, Definition, Implementation, and Close-out. Each gate is administered by a "functional unit responsible for specific actions and authorities in the approval process" and "all proposals must be approved at each gate in order to proceed further."[1]

It can take between 30 and 100 days, or more, to proceed from one gate to the next and scheduling of decision-making committees can also introduce delays. Assuming the minimum of 30 days per gate, the fastest a procurement could progress from Identification to an RFP, which occurs at the Definition Phase, is nearly seven years, though longer is common. There is a clear disconnect between the timelines of the decision-making cycle and that of the lifecycle of cyber technologies, which is 10 months or less. This decision-making process does not work for procurement officers or industry and consistently procures technological solutions years out of date.

1 Decision Making in the Capability Development Process: Organizational Issues within the Department of National Defence, Martin Rivard, Canadian Military Journal, 2018.

Allied cyber procurement practices also reflect the use of demonstrations, prototypes, and minimum viable products as viable bid submissions, which are prioritized over highly detailed and overly specified requirements. This is a new way for bidders to prove how they meet potential requirements, and can deliver functional solutions, before transitioning to full-scale deployment.

These emerging cyber procurement best-practices reflect a certain level of experimentation, and allow for different ways to promote greater competition while de-risking the procurement process for firms and governments alike. This point cannot be understated: modern approaches to cyber procurement have a different perspective on failure – a stepping stone, not a roadblock – along the path to successful acquisition. Modern procurement practices are also designed with the intention of allowing for greater flexibility in finding the balance between three mutually dependant factors:

1. Identifying, sourcing, and deploying new technologies at speed, which are available across a fast moving and highly innovative cyber ecosystem, to respond to cyber capability deficiencies;
2. Managing increasing system complexity and capability/technology integration requirements through a more equitable sharing in the ownership of integration risks and responsibilities between government and industry and;
3. Continuous alignment of capability development to operational intent through systemic and persistent end-user engagement throughout the procurement process.

10 Army Modernization Strategy, U.S. Army, 2019; Small Business Strategy, Department of Defence, 2019; Small Businesses Behind Defence's Biggest Projects Recognized, Ministry of Defence, 2018.

7.0 PROBLEM 3: PROCUREMENT PROFESSIONALS NEED NEW SKILLS

Modern approaches to cyber procurement demand the application of a diverse array of new and evolving skillsets. Procurement teams need to be comprised of professionals with a broad mix of proficiencies and capabilities including:

- Management of collaborative relationships between government and industry to maintain a shared and accurate understanding of the technical and operational problem spaces;
- The ability to forecast the implications of converging technologies and adjust procurements and projects in response;
- Allowing for new ways to showcase cyber solutions in a competitive environment and encouraging SME and startup engagement, including pitch competitions, x-prizes, and other emerging procurement practices;
- The technical competency to engage operators on real problems in a live or simulated threat environment to better understand implementation and interoperability concerns;

All interview respondents agreed that cyber procurement professionals will require access to ongoing training and skills-upgrading resources to keep pace with cyber innovations and with leading procurement practices and techniques.

For example, the U.S. military currently has more than 15 rapid-capability development and advanced-technology acquisition programs from Dragon's Den-style competitions and x-prizes, to dedicated venture capital investment funds.[11] This range of technological access points allows the U.S. military to access emerging technologies through a higher-risk approach where the risk is balanced across a portfolio of investments.

Additionally, some allied military academic institutions have developed curricula focused on advanced technology acquisition and integration in defence.[12] Canada may want to consider pursuing education and training partnerships with allied institutions to support the upskilling of its defence procurement professionals.

11 National Defence Authorization Act for Fiscal Year 2019, U.S. Congress, 2019.

12 For example, the Capability and Acquisition Practitioner Series at Shrivenham Defence Academy in the UK, or any one of the 100+ courses or digital learning engagements offered through the U.S.'s Defence Acquisition University.

8.0 IDEAS FOR REFORM

Although industry and government representatives interviewed for this report proposed many solutions to respond to cyber procurement's core challenges, consensus on which were most likely to lead to successful outcomes was not achieved.

However, experts across both the private and public sectors considered a few ideas worthy of further exploration and development.

IMPROVE THE SPEED AND FLEXIBILITY OF THE PROCUREMENT PROCESS

CGAI's 2020 procurement report developed three recommendations to improve DND-led procurements:

1. Sustain the flexibility to upgrade cyber capabilities over their life cycle by developing "evergreen umbrella projects for ongoing capability improvements where funding can be reallocated among sub-projects by project sponsors."
2. Develop a new Vote between Vote 1 and Vote 5 for high-technology acquisitions that has the flexibility of Vote 1 but the funding levels and ability to acquire new capability of Vote 5."
3. Develop a "fast-tracked approval and contracting process for technological and regulatory upgrades… with high flexibility in terms of initial budgets and schedules."[13]

INCREASE SUPPORT FOR EXISTING AGILE AND ITERATIVE PROGRAMS

Innovation for Defence Excellence and Security (IDEaS) is an agile innovation program that demonstrates some of the core characteristics of successful cyber procurement programs:

- Early-phase projects comprise bite-size requests for demonstration or proof of concept. Later phases increase the sophistication of the technological ask and scale of deployment;
- Prototypes and technology demonstrations are prioritized over paper-based submissions;
- Testing and validation phases are backed operationally and financially by military end-users;
- The program's staged progression from proof of concept, to prototype, to scaled testing, provides opportunities to re-evaluate and remove or engage new technologies and firms;
- Rewards are gated behind a progression of tangible deliverables that increase in complexity and cost, over time, minimizing the financial risks of failure for government and firms;
- The program's focus on outcomes, and willingness to consider a broad diversity of solutions from out-domain, significantly increases the solution space accessible to government;
- The program puts functional technology in the hands of CAF operators in less than a year.

DND, PSPC, and TBS should consider applying IDEaS' core characteristics to official cyber procurement programs. As Innovative Solutions Canada (ISC) shares many of IDEaS's core characteristics, ISED should work with client departments to make greater use of the program for national security and cyber challenges. Consideration should also be given to increasing the resources available to IDEaS's cyber component and developing a mechanism to fast-track winning projects into official DND/CAF procurement channels. The ability to launch classified IDEaS challenges is also likely worth further exploration.

RESPOND TO CYBER INTEGRATION CHALLENGES BY EXPANDING OPPORTUNITIES FOR EDUCATION AND TRAINING

> "Our current cadre of acquisition professionals have been taught to acquire capability in the context of discreet platforms. They have not been trained to bring several different technologies together, across a few different and complex technology areas. Nor have they been trained to assess their fit and interoperability within the existing platforms, capabilities, and technologies in the field."

The industry cyber experts interviewed identified two core training and education opportunities that could be optioned to help resolve the technology integration challenge:

- Embed acquisition professionals and establish two-way exchange programs with allied Material and Information Management (IM) organizations, U.S. Cyber Command, U.S. Rapid Capability Development Offices, and the Army Futures Commands, to gain first-hand experience working in programs acknowledged to be delivering successful cyber outcomes.
- Develop the mechanism for Canadian procurement professionals to receive undergraduate and graduate instruction through U.S. and UK military academic programs focused on advanced technology procurement and integration.

13 Toward Agile Procurement for National Defence: Matching the Pace of Technological Change, CGAI, 2020.

9.0 CONCLUSION: ESTABLISH A FORUM TO IMPROVE CYBER PROCUREMENT THROUGH COLLABORATION

The research conducted in support of this report demonstrates significant common ground between government and industry on the nature of the problems that are holding back cyber procurements in Canada. However, when it comes to solving these problems this report does not provide recommendations because none of the ideas presented have achieved government-industry consensus.

The ideas surfaced should instead be treated as the initial thoughts and early concepts percolating throughout Canada's cyber community. They may hold the potential to resolve some of the identified challenges, but they require further discussion and joint investigation by government and industry.

Progress hinges on the creation of a forum to structure a recurring dialogue between government and industry to jointly discuss and develop some of the potential solutions captured here, and to examine others.

Unsurprisingly, this is how many of Canada's allies stay on top in the cyber domain – through ongoing, institutionalized government-industry dialogue, knowledge sharing, and collaboration – aimed at gaining a sophisticated understanding of the rapidly changing, innovation-rich cyber domain to meet its risks and threats head on. Canada needs to do likewise.

The Cyber Advisory Council was instrumental in the development of this report and its recommendations, and is comprised of the following individuals:

AL AMLANI
GDMS Canada, Director Cyber Operations

ALLEN DILLON
root9B Canada, Chief Operating Officer

SHAUN COVELL
Sapper Labs, Director

CHRIS BARTLETT
CCX Technologies, President

NANDINI JOLLY
CryptoMill Cybersecurity Solutions, President and CEO

GEORGE AL-KOURA
ADGA, Director Cyber Operations

DAINA PROCTOR
IBM, Associate Partner, Security Intelligence and Operations Consulting

RAFAL ROHOZINSKI
SecDev, President and CEO

DAVE MCMAHON
Clairvoyance Cyber Corp., CEO

ROBERT MAZZOLIN
Rhea Group, Chief Cyber Security Strategist

TYSON MCCAULAY
Rockport Networks, Chief Security Officer

BILL DUNNION
Calian, Director Cyber Resilience

ABOUT CADSI

The Canadian Association of Defence and Security Industries (CADSI) is the national industry voice of more than 900 Canadian defence and security companies that produce world-class goods, services and technologies made across Canada and sought the world over.

The industries contribute to the employment of more than 60,000 Canadians and generate $10 billion in annual revenues, over 50% of which come from exports. To learn more, visit **www.defenceandsecurity.ca** and follow us on Twitter at @CadsiCanada.

Canadian Association of Defence and Security Industries

300-251 Laurier Avenue West
Ottawa, ON K1P 5J6

defenceandsecurity.ca
@cadsicanada