The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.07

An access to innovation program to enhance the technological capabilities of the armed forces

Marie-Pierre Raymond
MEng, CD (LCol Ret'd)
Defence Research & Development Canada (DRDC)
Ottawa, Ontario, Canada
e-mail: marie-pierre.raymond@forces.gc.ca

Eric Fournier
e-mail: eric.fournier@forces.gc.ca

Abstract. As part of "Strong, Secure, Engaged: Canada's Defence Policy" (Department of National Defence (2017) Strong, Secure, Engaged) released in 2017, the Canadian Department of National Defence (DND) announced the creation and implementation of an access to innovation program to be called the "Innovation for Defence Excellence and Security (IDEaS)" Program. The IDEaS Program was introduced to support, increase, and sustain science and technology (S&T) community capacity external to DND that can generate new ideas and formulate solutions to Canada's current and future defence and security innovation challenges. This paper will explore the design of this new business model through the delivery of the first proof of concept to have gone through the whole IDEaS cycle, in order to showcase the validity of this concept and processes. It also demonstrates that IDEaS has allowed a closer relationship with innovators and firms that had never worked with the defence industry, as well as the identification of novel solutions to a host of problems/challenges facing defence and security.

Keywords: technological capabilities, IDEaS, innovations, SOAR, defence capability.

Introduction

Accessing innovative solutions to support defence and security needs is crucial for Canada to stay technologically advanced, enhancing security capabilities, and addressing the dynamic threats landscape. It is essential to stimulates the development of cutting-edge solutions, promote strategic advancements, and ensure Canada maintains a competitive edge in the ever-changing landscape of defence requirements and security needs. In response to this complex environment, Canada launched the Innovation for Defence Excellence & Security (IDEaS) program, with the goal of augmenting the Department of National Defence (DND) and the Canadian Armed Forces (CAF) capabilities. Several allied nations have initiated comparable innovation programs to encourage non-traditional defence innovators to actively engage and provide their technologies for defence applications. These programs, such as the Defence Innovation Unit (DIU) and SOFWERX in the US, the Defence and Security Accelerator (DASA) in the UK, and the Defence Innovation Hub in Australia, use a very similar general business model than the IDEaS program but with various specificities in their applications. The IDEaS program represents an investment in access to Canadians innovators to enable Canada's military to tap into the nation talent pool more efficiently. IDEaS is built on three fundamental pillars: recruiting innovators (connect), supporting development (develop), and maturing innovative solutions toward adoption (evaluate).

IDEaS was announced in the Fall of 2017 in Strong, Secure, Engaged (SSE), Canada's defence policy. The program officially launched on April 9th, 2018. This innovation program has been given $1.6B CAD over 20 years to deliver on its mandate and advance defence capabilities. The goal is to continuously tap Canadian innovators for their solutions through various calls for proposals

launched on a regular basis. IDEaS is for all Canadian innovators, from defence primes to academia, small and medium sized enterprises to not-for-profits, municipal / provincial / territorial entities to individuals.

Program design

This novel program acts as a facilitator between the DND/CAF capability requirements and the Canadian innovation ecosystem. Any organization within DND/CAF can generate and submit a priority/challenge to the IDEaS team, from the Army to the Air Force, to Space, to Cyber and all the other organizations of the department. Following a prioritization of the DND/CAF priorities received by the program (a prioritization process is required as too many priorities are received from DND/CAF), the IDEaS team turns each priority into a challenge to be released to the innovation community.

The program is intended to help foster solutions at any stage of development that have potential defence and security focus and align with DND/CAF priorities. From early research and development to prototyping and testing novel concepts generated by innovators, the program exists to advance technology. DND will access the extraordinary talent and ingenuity of innovators across Canada, including non-traditional players, seeking to leverage and integrate their expertise. Innovators, in turn, will gain DND's support through funding and guidance to help create capability and capacity for defence and security.

Each challenge released by IDEaS represents a genuine and current need from a number of Canadian defence and security stakeholders. Challenges are written with broad language intentionally to encourage a higher volume of submissions, as it is expected that this will lead to the discovery of novel and unexpected proposals. It should be noted that since the launch of the program in April 2018, the program has addressed more than 75 challenging problems spanning various defence and security domains, including electronic warfare, counter-UAS, communications in denied environments, ISR, human performance, cybersecurity, transition from military to civilian life, as well as quantum technologies, artificial intelligence based-technologies and many more.

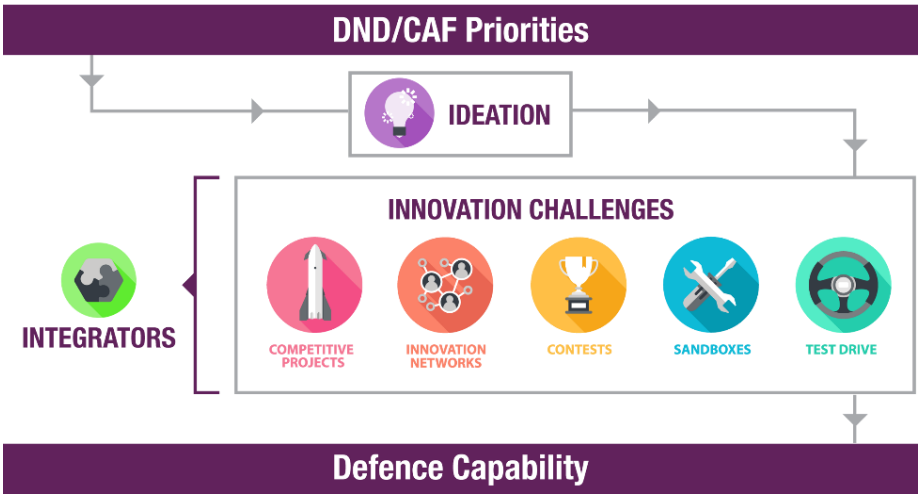


Figure 1: IDEaS Elements that enable the search of new capabilities for DND/CAF

IDEaS Elements

IDEaS leverage 5 different elements to access innovation depending on the technical readiness level of the solution and the types of outcomes sought by the DND/CAF partner.

Competitive Projects – This element was the first one developed under the program, and it

is still the work horse of the program: more than 75% of all the challenges launched by IDEaS so far have been with this tool. The Competitive Projects element funds projects fast. It advances promising technology quickly through a phased approach, which can quickly move technology ahead. Projects that show promise are considered for additional phases of funding.

Contests – Contests are a competitive means of finding innovative solutions and awarding prizes to the best solutions derived from the innovation community. Whether it is a hackathon, a pitch event in front of military experts, or an amazing race, Contests will bring innovators face-to-face with the competition. Depending on the challenge, Contests could entertain solutions at various Technology Readiness Levels, but it is expected that most of the actual events are going to be directed at higher Technological Readiness Level (TRL) (NASA (2023) Technology Readiness Levels) solutions.

Innovation Networks – Innovation Networks are an opportunity to create new networks (or support existing networks) of understanding, stimulate collaboration and allow for the free flow of ideas critical to innovation. They usually occur at lower TRL level, so to allow fully creative solutions to be generated by the participants and support basic and applied research, analysis, technology development and knowledge transfer leading to innovative solutions.

Sandboxes – A Sandbox is an opportunity for innovators to test and demonstrate their prototype solutions to National Defence military users and science experts for a specific IDEaS advertised challenge. The IDEaS team also provides on-site military and science experts, as well as other government safety and security potential users, to give innovators observational feedback on their solutions.

Test Drive – Test Drives takes an innovative solution through the final stage of the innovation journey towards commercialization. The IDEaS Team acquires a solution so that DND/CAF can assess the readiness of the product in a real-world environment for a military audience. Innovators will receive feedback on their technology following the testing.

In addition to these 5 "access" elements, another very important element for the innovator community is called "**Integrators**". Although not directly linked to the call for proposals process, like the previous five elements, it is really an enabler for the innovators. This element has been developed to provide constant support and oversight to the innovators, by providing scientific and operational experts for every challenge launched. These experts come from DRDC and DND/CAF and are experts in the specific domains of each challenge. Their role is to provide guidance to the innovators, without orienting their work towards specific solutions as the role of the program is to allow innovators to develop their own novel and innovative solutions.

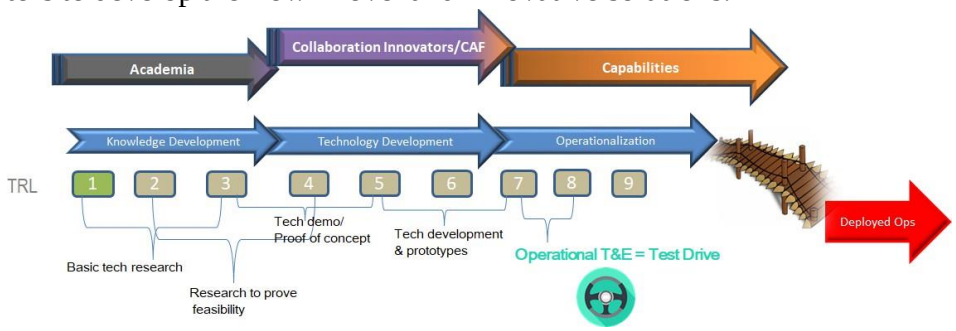


Figure 2. IDEaS innovation pipeline to transform innovation into new capabilities for DND/CAF.

Finally, IDEaS innovation champion, called **Challenge Managers**, are assigned to every challenge launched by the program. These defence scientists are responsible for organizing and

overseeing CAF innovation challenges as they move through the IDEaS innovation pipeline. Their role is to create an environment conducive to innovation supporting the innovators and the CAF stakeholder. They provide guidance, support, and expertise to individuals and teams.

IDEaS PROOF OF CONCEPT

In April 2018, the IDEaS program, and members of the CAF Director General Information Capabilities Force Development (DGICFD) organization collaborated on one of the first challenges launched by the program. They worked on the formulation of the challenge statement of a cybersecurity hard problem that was titled "**Cyber Attribution for the Defence of Canada**".

A. Challenge Development

The Challenge scoping was done with subject matter experts from the organization that submitted the Challenge and defence scientists supporting the organization. It was a collaborative endeavor aimed at defining and refining the parameters, objectives and boundaries of the challenge/hard problem that needed to be addressed. The process involved brainstorming, discussion, analysis to ensure that the challenge was well-defined, aligned with the goals of the organization and of course actionable by the innovator. "Attribution" is one of the most challenging problems in cyberspace. The decentralized, dynamic, and open architecture of the internet enables a perpetrator to easily hide his or her tracks and operate with varying degrees of anonymity.

Following the challenge development process, the Challenge Statement was written as:

The Department of National Defence (DND) is looking for innovative approaches to access, interpret, and compare all available evidence (e.g., technical, all-source intelligence) on how current cyberspace activities get attributed. This will assist in assessing the current cyberspace environment to improve methods on how to obtain secure cyberspace attribution in a timely manner.

The desired outcome of this research effort is to demonstrate methodological approaches and confidence metrics as well as identify challenges and issues (for e.g., technical, regulatory, etc.) with cyber activity attribution that would advance shared understanding of cyberspace and promote national cybersecurity.

B. Calls for Proposals.

An innovation call for proposals (CFP) was the next steps in the process. It was conducted through a structured process to solicit ideas and solutions from Canadian innovators. Following the reception of the proposals, a review, evaluation, and selection process was completed to identify the best proposals for funding. Criteria such as Merit, Novel & Innovation, Impact, Feasibility, Operational Investment and Advancement of the solution were used throughout this process. A total of 24 proposals were received for this CFP, which allowed 7 of these to be selected for the initial phase of funding under Competitive Projects. This original phase of funding has for objectives to establish the merit, innovativeness, and impact of the solutions to address the specific defence and security challenge stated above.

C. Progress through Competitive Projects

Moving along the IDEaS process, one proposal (one out of the 7 chosen for the first phase of funding) was selected for the next phase of funding – only one proposal was selected by the Stakeholders to move forward and receive further funding, and it was the proposal from Sapper Labs (a small & medium enterprise). The solution was to address both strategic issues and next-generation operational solutions. Sapper Labs was proposing to build a next-generation cyber threat hunting system with accelerated detection, attribution and active cyber defence through automated playbooks, Security Orchestration, Automation and Response (SOAR) on forward deployed networks in conflict zones. It offered an innovative way to hunt down bad actors and confidently assign attribution for their actions which was never done before. It was therefore selected to continue its development under the second phase of funding of Competitive Projects.

D. Test Drive

After successfully delivering under the Competitive Projects development phase, Sapper Labs were granted a $7.5M CAD contract for the program's first "**Test Drive''**, the last component of the IDEaS innovation pipeline. In using the funding received from the Competitive Projects, Sapper Labs were able to develop a cyberprotection platform capable of identifying the perpetrators of sophisticated cyber threats. Therefore, the objective of the Test Drive was to validate their cyber attribution capability in a DND/CAF operational setting to accelerate the detection of advanced threats against Canadian assets and led to the development of the Canadian Active Cyber Defence Platform (CACDP) tool to the CAF. The Test Drive in CAF operations lasted 18 months and was broken-down into four phases:

Phase 1 – Initialization and Implementation of the CACDP; Phase 2 – Systems Integration, Tuning and Training analysts;

Phase 3 – Conduct of Cyber and Intelligence Operations and Testing; and Phase 4 – Cognitive Warfare Proof-of-Concept.

Operationalizing the designs and methodologies in this project was critical to achieve the cyber objectives of the Strong, Secure, and Engaged Canadian Defence Policy. During the Test Drive, the following activities were planned to be performed on an operational network or forward-deployed deception network at scale:

- Automate/accelerate attribution of advanced persistent threats and launching of active defence (using AI/ML);
- Integrate/fuse cyber threat intelligence (CTI), Open Source Intelligence (OSINT) and Commercial Sourced Intelligence with real time network sensing to support attribution; and
- Orchestrate threat hunting, intelligence production and active cyber defence. Development of targeting packages and demonstrating the ability to take action based upon playbooks.

Sapper labs accommodated a substantial number of feature requests from the operators during the live operations part of the experiment. Innovator flexibility was critical to address end-users evolving needs as the Test Drive progressed and the real-time threats evolved. At the same time, Sapper Labs, being the first innovator to reach this Test Drive milestone, had to overcome many unforeseen situations including security issues, approbations periods, etc.…

Sophisticated threat actors blended offensive cyber–cognitive campaigns as part of an informationized warfare strategy. In the course of this project, CAF operators using Sapper Labs Active Cyber Defence Platform (CACDP) detected cyber and cognitive attacks against the CAF attributed to Russia - specifically, APT28 Fancy Bear, STRONTIUM Russian cyber espionage group associated with the Russian military intelligence agency GRU Unit 26165 and Unit 74455, as well as the Internet Research Agency (IRA). Sapper Labs discovered direct threats to CAF attributed to these entities (this information can be found in Sapper Labs final report and is open source).

E. Follow-Up and Opportunity from working with IDEaS

Participating to this challenge and working closely with the CAF opened additional opportunities for Sapper Labs to collaborate with other advanced innovators working in the cyber domain. In June 2021, NATO, in partnership with IDEaS and the Canadian Special Operation Forces Command, released an Innovation Challenge looking for innovative concepts and/or tools for countering cognitive warfare. The goal of the challenge was to look for technics and tools to identify, assess, and protect against attacks on the cognitive domain of NATO forces and their allies. This pitch style event invited non-traditional thinkers from across all 30 NATO member nations to showcase ways of securing the cognitive domain against attacks. Following the NATO competition, Sapper Labs collaborated with the overall winner, the US innovator Veriphix (NatSec technology that directly tracks population level belief using a low signature active and ethical data collection) and the recipient of the best Canadian-made solution BMU (Counter-Disinformation Intelligent Solution (CDIS) focusing on the Sense – Augmented Intelligence platform) to initiate a research project focused on countering Russia disinformation and cognitive warfare tactics. The development

and trial of this Cognitive Warfare phase lasted approximatively 4 months.

Cognitive warfare, intelligence and targeting of private military contractors became highly-relevant to this challenge (Cyber Attribution Sophisticated Threat Actors in the Defence of Canada). Hence, they represent a significant part of this project using the Proof-of-Concept for Cognitive Warfare.

Intelligence analysis showed that adversaries transition seamlessly from cyber and cognitive domains. In fact, it is no longer possible to separate cyber and cognitive warfare. Nation-state actors like Russia outsource development and operations to a vast network of security companies, dis-information centres and Private Military Contractors. Target systems analysis revealed direct connections between these entities and blended cyber-cognitive operations against Canada.

In partnership and embedded with military operational units, Sapper Labs delivered an advanced, innovative and effective cyber defence, cognitive warfare, intelligence and targeting solution to CAF. All objectives of the IDEaS Operational Test were fully met. Additionally, several other remarkable and important achievements were accomplished through the execution of this program related to cyber defence, strategic intelligence, operational intelligence and cognitive warfare.

Conclusions

IDEaS does work. After more than 5 years using the Innovation for Defence Excellence and Security (IDEaS) program and tools, DND/CAF deciders and staff can confirm that this business model can work. IDEaS has allowed a closer relationship with innovators and firms that had never worked with the defence industry, as well as the identification of novel solutions to a host of problems/challenges. The experience of IDEaS, with over 75 challenges since the beginning of the program in 2018, covers all of the most defence/security domains of work, such as protection, electronic warfare, communications, human performance, transition from a military career to civilian life, quantum and AI, and many more. Novel solutions are being generated in many of these domains of work.

The success of the IDEaS Challenge “Cyber Attribution for the Defence of Canada” can be attributed to three observations:

- Effective innovation program – IDEaS is a critical CAF program for both innovation and capability development, at speed, particularly in cyber, cognitive warfare and intelligence domains. It is a great program for positive Canadian outcomes;
- Operational outcomes - The relationship between Sapper Labs, CAF operators and IDEaS management was relentlessly focused on timely mission outcomes, despite challenges; and
- Collaboration breeds better innovation - through execution, Sapper Labs and CAF became more capable innovators and operators. They became allies in meeting complex challenges and realities for operational missions – from policy, to doctrine, operational planning, execution, and training. Successful technology adoption was directly correlated to mutual knowledge transfer.

References

1. Department of National Defence (2017) Strong, Secure, Engaged: Canada’s Defence Policy. Retrieved 8 December 2023. Strong, Secure, Engaged: Canada's Defence Policy - Canada.ca DND/CAF
2. NASA (2023) Technology Readiness Levels. Retrieved 12 February 2024. https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/ Manning, Catherine.