



DEFENCE MARKET ACCESS SERIES

Speaking Defence

How to position your technology to show value for defence buyers

Webinar 2

July 16, 2026

We are grateful to the people of the x^wməθk^wəy^əm
(Musqueam), Skwxwú7mesh (Squamish), and
Selílwitlh (Tsleil-Waututh) Nations for sharing
and stewarding these lands.



Musqueam
First Nation



Skwxwú7mesh
Úxwumixw
Squamish Nation





THE SERIES

A journey into Canada's defence market

Five sessions. DIGITAL convenes, the credibility comes from across the ecosystem.

1

Getting In the Door

How to enter the market

RECORDING AVAILABLE

2

Speaking Defence

Positioning your tech for buyers

WE ARE HERE

3

How Money Moves

Funding & procurement mechanisms

4

Working with Primes

Prime relationships, ITB & content

5

Partnerships & IP

Alliances while protecting IP

After the series: *select participants may be invited to closed, invitation-only Defence Showcases with buyers and primes.*



WHO'S IN THE ROOM

A quick read of the room

A snapshot of who has registered: skews early, with most still scoping whether defence applies to them.

221

Registrations (as of Jul 15)

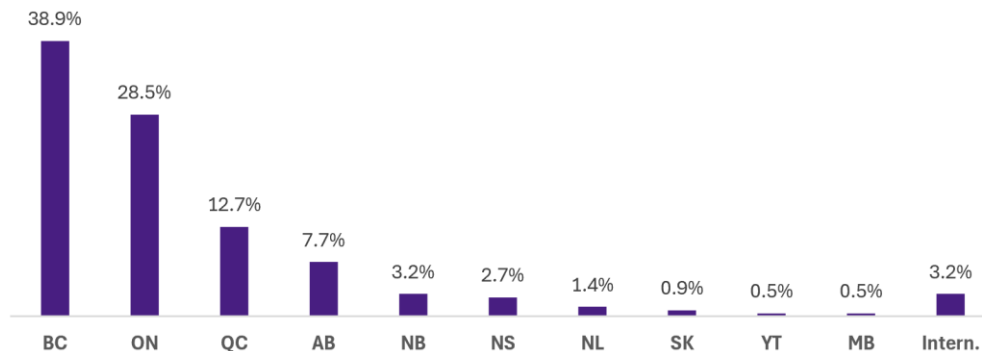
54%

are companies with technology,
product, or service

68%

of companies are under \$2M
revenue (incl. pre-revenue)

📍 REGISTRATIONS BY LOCATION



MODERATOR REMARKS



Genevieve Bonin

DIGITAL Executive
Senior Advisor



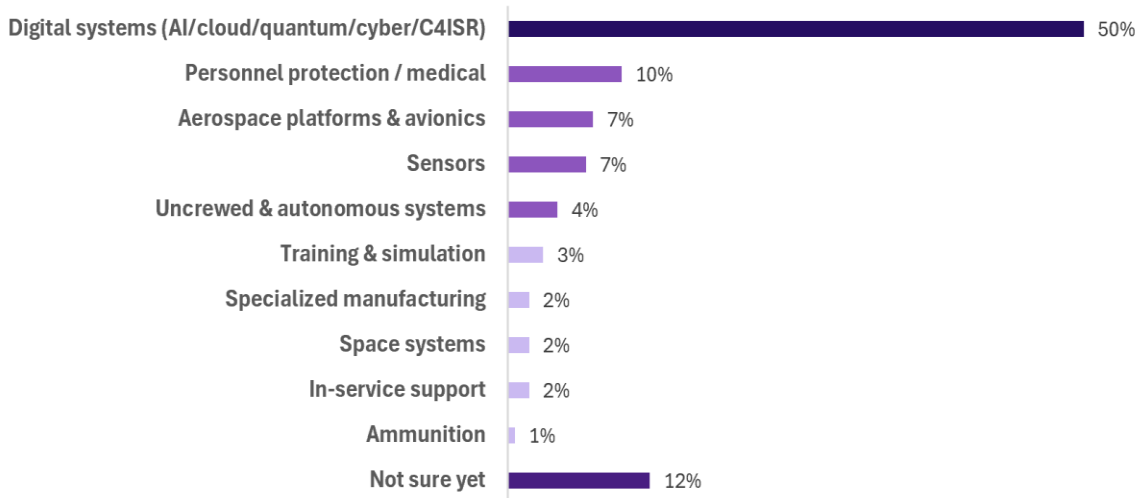
WHO'S IN THE ROOM

A quick read of the room

Half the room specializes in digital systems, with the majority offering enabling, non-core dual-use solutions

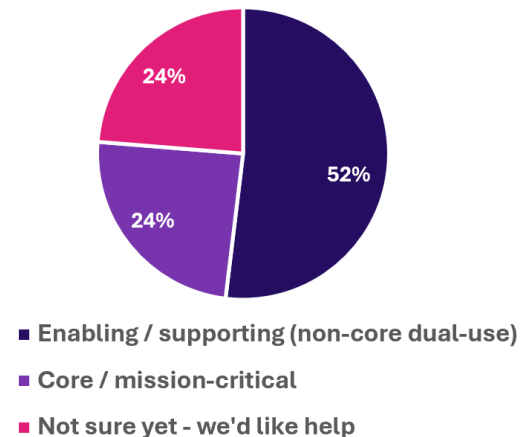
ALIGNMENT TO SOVEREIGN CAPABILITIES

Share of capability responses (n = 162)



SOLUTION'S ROLE IN DEFENCE

Share of role responses (n = 156)



GUEST SPEAKER



Ron Lloyd

Vice-Admiral (Retired), Senior Associate, Tactix



DEFENCE MARKET ACCESS SERIES · WEBINAR 2 · JULY 16, 2026

Speaking Defence

The language, structure, and unwritten rules of Canada's defence world.

Ron Lloyd Vice-Admiral (Retired), Senior Associate, Tactix

THE OPERATING MODEL

Operating at the speed of trust

In defence, credibility is earned. Relationships move faster than paperwork – and first impressions carry more weight here than almost anywhere.

1 Trust is scarce

Defence barely trusts its own services or other departments – you can imagine how much they trust industry

2 Mostly familiar

~80% of defence processes mirror industry; the distinctive 10–20% - the battlespace – is what they stress.

3 Speak the language

Without their vocabulary, priorities, and operating models, it's hard to be taken seriously.

4 Relationships first

“Speed of trust” is about people. Invest early – first impressions are hard to reset.

THE LANDSCAPE

The defence ecosystem

Three broad groups shape how defence buys, partners, and delivers.

Government

- Department of National Defence (DND)
- Canadian Armed Forces (distinct from DND)
- Defence Investment Agency — inside Public Services & Procurement Canada
- Shared Services Canada

Alliances & partners

- NATO — 32 nations
- Five Eyes — US, UK, Australia, NZ
- NORAD — the world's only binational command (US / Canada)
- AUKUS (Pillar 1, no Canada) · Indo-Pacific (+ Japan, South Korea)

Other actors

- Original Equipment Manufacturers (OEMs)
- In-service support (ISS) providers
- Academia
- Small & medium enterprises (SMEs)

WHO'S WHO

How defence is organized

One minister, two components. Civilians lead on policy and budget; the military leads on operations.

Minister of National Defence

Civilian component

Department of National Defence (DND)

Deputy Minister(s) · Assistant Deputy Ministers

Leads on **policy and budget** – the professional public service.

Military component

Canadian Armed Forces (CAF)

Chief of the Defence Staff · Service Chiefs

Leads on **military operations** – from planning to completion.

Referring to both together? **“Defence”** is the collective term for DND / CAF.

READING THE ROOM

Ranks and “Equivalencies”

A rough map between military rank and civilian seniority — useful for knowing who you're talking to.

Military	Civilian equivalent
General / Admiral (4-star)	Deputy Minister (DM)
Lieutenant-General / Vice-Admiral (3-star)	Assistant Deputy Minister (ADM)
Major-General / Rear-Admiral (2-star)	ADM / Director General
Brigadier-General / Commodore (1-star)	Director General
Colonel / Captain, Navy (4-ringer)	Director
Lieutenant-Colonel / Commander (3-ringer)	Section Head

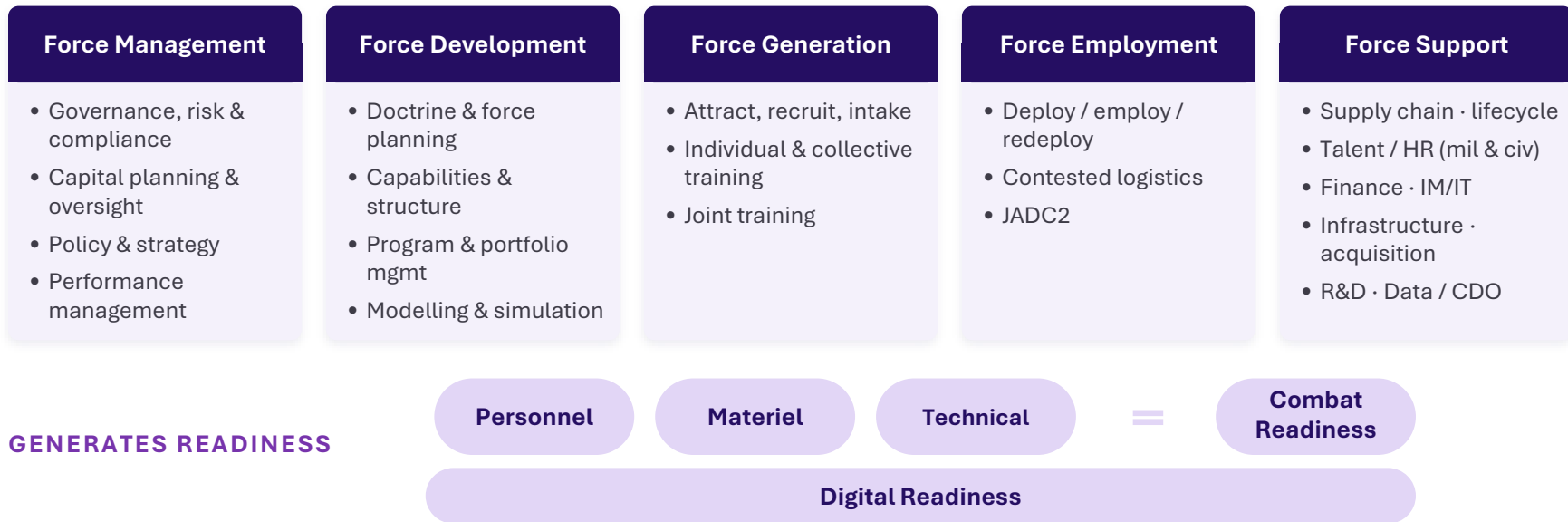
Watch-outs

- “Commander” is both a rank (3-ringer) and a position (e.g. Commander of the Navy, a 3-star).
- The Army has a 2-ring Captain; the Navy a 4-ring Captain – and “Captain” is also the ship's role, any rank.
- “Admiral” and “General” refer to all officers at that level, even though each is also a specific rank.

HOW DEFENCE RUNS

5-F model and Readiness

Five “force” functions work together to generate readiness



THE CORE IDEA

What we mean by Command & Control (C2)

Command & Control is about **making and executing decisions faster than our adversaries.**

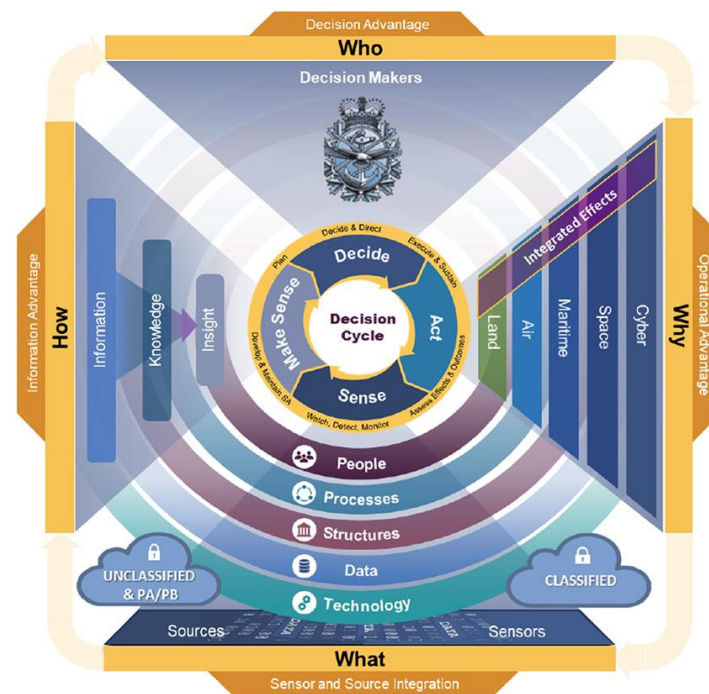
Canada and US

PDC2

Pan-Domain Command & Control – Canada's framework, tailored to CAF operations.

CJADC2

Combined Joint All-Domain Command & Control – the US vision for linking sensors and shooters across every domain.



HANDLING INFORMATION

Security classification frameworks

Allies use different tiers for the same idea. Know the local system before you share.

Canada

- Protected A
- Protected B
- Protected C
- Confidential
- Secret
- Top Secret

United Kingdom

- Official (Sensitive)
- Secret
- Top Secret

Australia

- Official (Sensitive)
- Protected
- Secret
- Top Secret

United States

- Controlled Unclassified Info (CUI)
- Confidential
- Secret
- Top Secret

Clearances ≠ classifications. A clearance lets a person access classified information – its title often differs from the data's label and is managed per country. In Canada the clearances are Reliability, Enhanced Reliability, Confidential, Secret, Top Secret, Enhanced Top Secret.

Levels of war vs. industry language

Three levels connect national strategy to the front line — and map onto how industry talks about scale.

Strategic

Sets direction and strategy. Think NDHQ / the Pentagon.

Operational

Joins strategy to tactics. Canadian Joint Operations Command (CJOC); US Geographical Commands (e.g. NORTHCOM).

Tactical

Acts in the battlespace. Individual units carrying out the mission.

“Enterprise to the tactical edge” captures the goal of seamless digital enablement across all three levels.

KNOW YOUR BUYER

The maturity of the client

Defence experts are deep in their profession – but rarely in bureaucracy or industry. Calibrate your expectations.

- 1 Experts in their field** Generals & Flag Officers (GOFOs) know their profession deeply – not navigating government or reading industry.
- 2 Risk flips by setting** The military is risk-tolerant in the battlespace and risk-averse in bureaucratic frameworks.
- 3 Policy drives caution** That aversion is codified in “small-p” policies – non-legislated policies, guidelines, directives, and tools.
- 4 Limited industry view** Very few military or public-service staff are aware of industry best practices.
- 5 Procurement decides** In almost all cases, procurement officers have the final say on the deal.

GUEST SPEAKER



Derek Dobson

Partner, Defence and National Security,
IBM

A person wearing a helmet and goggles is looking through the open hatch of a military vehicle. The scene is set in a desert environment with rocky ground. The image has a dark, muted color palette.

Talking Defence

Derek (Degs) Dobson
Partner, Defence and National Security

Defence Modernization in the Era of AI

Strategic Context:

ONSAF, DIS, DND/ CAF Data and AI Strategies emphasize the need for:

- AI that accelerates targeting and delivers decision advantage
- Integrated platforms, sensors, data and CSISRT applications across all domains – and between allies
- Governance, auditability and sovereign control of data and operational capabilities
- Trustworthy, autonomous systems
- Zero trust and Data Centric Security Systems

Critical Insight:

Commercial dual-use technologies refresh every 12-18 months while defence procurement cycles for digital capabilities average 3-5 years. This mismatch creates strategic vulnerability.



Defence Leader Perspectives



The Challenge

FVEY and NATO Priorities are Clear But Progress is Uneven

Commanders' positive view
of where operational
advantage can be gained:

- 98% - Secure and Interoperable C5ISRT
- 98% Information operations
- 98% Cyber operations
- 97% Integration of AI and Autonomous platforms on Operations
- 94% Sustainment and Logistics

The Insight

Stuck in Pilot phase

Success in implementing
solutions:

- 20% in Secure and Interoperable C5SRT
- 12% in Information operations
- 25% in Cyber operations
- 15% Integration of AI and Autonomous Platforms on operations
- 15% In Sustainment and logistics

Takeaway

Progress stalls unless solutions are:

- Recognized as essential at all leadership levels
- Embedded into institutional and operational systems
- Supported by modern infrastructure and data platforms
- Governed properly
- Have clear – mission focused ownership

The conditions that shape success



The Challenge

System readiness is a strategic chokepoint

- Across NATO and FVEY fewer than one third of enterprise of operational applications, and systems are ready for AI and Automation
- Acquisition and authorization cycles are twice more than twice as long as development cycles
- Organizations that are highly reliant on external providers show slower progression towards operationalized solutions.

The Insight

AI foundations = strategic infrastructure

Leaders prioritize the following as national priorities to mitigate strategic risks:

- 67% Data Sovereignty
- 66% Cybersecurity
- 62% regulatory and policy frameworks
- 56% Digital Infrastructure
- 54% innovation ecosystem
- 54% Education and workforce development

Takeaway

Risk mitigation is more important than risk avoidance

AI & Automation readiness for the military is matter of national infrastructure, not just organizational optimization.

Building resilience, sovereignty, and interoperability now requires deliberate choices - about what to control, what to share, and what to standardize across defence enterprises and alliances.



1 Modernize core systems so AI operates inside real workflows.

Solutions cannot deliver value when insights remain outside operational and enterprise systems. Be prepared to deal with Legacy platforms, fragmented architectures, and brittle integrations.

2 Treat data readiness as an ongoing operational discipline.

Anticipate the need to clean, govern it effectively. Interoperable data flows must be continuously maintained as part of daily operations. One-time data initiatives do not sustain performance or trust at scale.

3 Help defence build durable internal capability to strengthen operational resilience

Sustainable tech adoption depends on developing in-house skills, institutional knowledge, and lifecycle ownership across data, models, and systems. Internal capability ensures continuity, adaptability, and control when operating conditions change or external support is constrained.

4 Get leadership support to force the transition from pilots to mission-relevant deployment

Initiatives must move decisively beyond experimentation and be embedded into priority work-flows with clear ownership, measurable outcomes, and operational accountability.

5 "Design in" trust, oversight, and human accountability by design

Explainability, auditability, and clear human responsibility must be built into systems from inception—especially as autonomy and decision impact increase

Defence Market Access Series



Speaking Defence:

How to position your solution to show value for defence buyers



Genevieve Bonin

DIGITAL Executive
Senior Advisor (Moderator)



Ron Lloyd

Vice-Admiral (Retired), Senior
Associate, Tactix



Derek Dobson

Partner, Defence and National
Security, IBM



Daly Brown

Co-Founder & CEO, Metropolitan
Technologies



Driving real results for Canada.



[DIGITAL dual-use portfolio](#)



Artyom Mamzhiev

Senior Innovation Strategist (Dual-Use Lead)



amamzhiev@digitalsupercluster.ca