Closing the gap

In modernizing NORAD, digital integration could be the most pressing and pivotal challenge of all

By Grant McDonald and Dan Doran

The April 2024 defence policy update (DPU) was very clear about purchasing priorities over the next few years: strengthening foundations by way of materials reinvestment in addition to pursuing the development of new capabilities in High Arctic security, missile defence and cyber.

These priorities have been supported through specific programs and planned funding, albeit over 20-years, for programs related to northern operational support hubs and a satellite ground station in the Arctic. This is in addition to billions being earmarked to build out a new global satellite system and a joint cyber operations capability, and to acquire long-range missiles, maritime sensors and airborne early warning aircraft—all while investing to keep existing platforms operational until their fifth-generation successors come online in the next decade.

These commitments build on the $38.6 billion already allocated to northern defence that came out of the Strong, Secure, Engaged (SSE) defence policy to meet Canada's collective NORAD obligations. While criticism has been levelled that the promised spending doesn't begin until 2026, these commitments matter—especially given the dearth of policy focus on digitization and integration in SSE. The DPU goes a long way in closing the gap.

Posture centric

Given all this arguably positive news for NORAD modernization and northern security in general, what's less clear is how these numerous weapons and sensor platforms are going to be synchronized to create a fully integrated digital decision-making 'system of systems' that can effectively address the threat profiles we currently face in addition to the AI-enabled threats of the future.

DND leadership won't be surprised by this observation, having been seized by the 'how' ever since answering the 'why,' in equal parts through the Digital Campaign Plan (DCP) and, more recently, the CAF AI Strategy.

Moreover, DND has also identified the desired end-state of its ambition to achieve full digital integration through the second line of effort in the DCP—specifically, to "Design, build, and field Pan-Domain Situational Awareness (PDSA) tools and concepts that integrate all domains." This will require the transformation of current operational concepts toward an orchestration of activities that transcend domains, promote pan-domain thinking and integrate the overlap among domains to promote integration by design—all through employment of the National Defence Operations and Intelligence Centre as the vehicle of operationalization, command and control.

These are all good signs. However, the next steps in the digital integration journey is where the path can become winding, treacherous—and costly.

Far from effortless

Achieving digital integration will require the application of a slightly modified version of the five lines of effort detailed in the AI Strategy, with the success of each line being inextricably linked to the success of the others:

- Fielding and employing digitally grated capabilities.
- Rigorously applying organizational change management and business transformation.
- Embedding resilience and reliability across systems.
- Recruiting the right talent and training them efficiently and effectively.
- Partnering across stakeholder departments and transformational engagement with industry.

These are the guideposts that, while not eliminating risks along the digital integration journey, will keep the organization on track toward the final objective of PDSA. And while each of them would be worthy of their own article, it's worth zeroing in on a couple of the more challenging areas.

Organizational change management (OCM) and business transformation (BT)

Both are distinct practices, but they are also very much intertwined in planning and execution. Digital integration will have to overcome all the same OCM challenges outlined in the AI Strategy related to working horizontally, embracing disruption and being adaptable. These mindsets will be required to navigate the process changes that will come with digital integration of platforms upgraded from, in some cases, technology from the 1970s and 80s—the equivalent of going from a Commodore 64 to a smartphone.

Partnerships

This will also be a difficult gap to cross, requiring a reimagination of the trust relationship between DND, other government departments and industry. Building bridges will require all stakeholders to take risks and actively nurture the kinds of professional and transformational connections that can generate the trust needed to foster creative solutioning and fight through these challenges.

Known unknowns

Ben Horowitz includes in his book, *The Hard Thing About Hard Things*, a couple of insights related to his lifetime of experience as a serial tech entrepreneur. The first one speaks directly to digital integration: "hard things are hard because there are no easy answers or recipes." The second one speaks to addressing the first and should be a mantra among the leaders who are tasked with eating the digital integration elephant: "It's a good idea to ask, 'What am I not doing?'" This is what we encourage senior leadership in the armed forces, government and industry to collectively consider.

Grant McDonald is the Global Aerospace and Defence Industry Sector Leader at KPMG International. **Dan Doran** is the Canadian Defence and Security Sector Leader at KPMG in Canada and a CAF veteran. For more information, visit, www.kpmg.ca. The views expressed here are their own and do not necessarily reflect a CDR editorial position.

Contact us

Grant McDonald

Global Sector Leader,
Aerospace & Defence
KPMG in Canada
246-434-3900
grantmcdonald@kpmg.ca

Dan Doran

Director, Public Sector Solutions,
Advisory | Practice Lead Defence and Security
KPMG in Canada
613-845-2064
dandoran@kpmg.ca