CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE

FORCE DEVELOPMENT

Digital Transformation in the Canadian Armed Forces

Report - December 2024

FORCE DEVELOPMENT

Digital Transformation in the Canadian Armed Forces

Roundtable

Report - December 2024

On the Cover

Top - Left
Combat Camera / Flickr
“HMCS VICTORIA at Sea”
Photo by LS Zachariah Stopa, MARPAC Imaging Services

Top - Left of Centre
Combat Camera / Flickr
“Operation PROJECTION”
Photo by Corporal Connor Bennett, Canadian Armed Forces Photo

Top - Centre
Combat Camera / Flickr
“Indo-Pacific Deployment 2023”
Photo by Aviator Gregory Cole, Canadian Armed Forces Photo

Top - Right of Centre
Combat Camera / Flickr
“Operation SAVANNE”
Photo by S1 Taylor Congdon, Canadian Armed Forces Photo

Top - Right
Combat Camera / Flickr
“Exercise RIMPAC”
Photo by Sgt Marc-André Gaudreault, Valcartier Imaging Services

Bottom - Left
Combat Camera / Flickr
“DP3 Bravo Platoon Commander Course”
Photo by LS Zach Barr, Canadian Army Trials and Evaluations Unit (CATEU) Gagetown

Bottom - Left of Centre
Combat Camera / Flickr
“INDO-PACIFIC DEPLOYMENT 2023”
Photo by Aviator Gregory Cole, Canadian Armed Forces Photo

Bottom - Centre
Combat Camera / Flickr
“Operation REASSURANCE 23-02”
Photo by Captain Joffray Provencher, eFP BG Latvia Public Affairs and Imagery Section, Canadian Armed Forces Photo

Bottom - Right of Centre
Combat Camera / Flickr
“Exercise REFLEXE RAPIDE”
Photo by Corporal Djalma Vuong-De Ramos, Canadian Armed Forces photo

Bottom - Right
Combat Camera / Flickr
“Exercise RESILIENT RESOLVE”
Photo by MS Steeve Picard

Introduction

In recognition of the complexity of sustaining defence capabilities, including through timely defence procurement, the CDA Institute initiated the Force Development Series to bring together subject matter experts from across academia, government, industry and serving and retired military members for open and frank roundtable discussions. These events facilitate multistakeholder, solutions-focused dialogue and expert analysis on pressing challenges affecting the Canadian Armed Forces' readiness and capabilities.

This report summarizes the discussions held during a CDA Institute roundtable on 'Digital Transformation in the Canadian Armed Forces' on December 6, 2023. It provides a comprehensive overview of the key points made by the invited experts. The report aims to promote better understanding and informed debate about the challenges associated with sustaining this critical capability for Canadians. Complying with the Chatham House rule, the report does not attribute any comments to individuals.

Executive Summary

In 2022, the Department of National Defence (DND) published the *Canadian Armed Forces Digital Campaign Plan* to chart a path for the digital transformation of the CAF in recognition of the fundamental ways in which digital and emerging technologies continue to alter the profession of arms. However, despite having developed a detailed strategy for digital transformation, the CAF has struggled with its implementation. The persistent inertia around digital initiative implementation across government speaks to the reality that Canada is ill-adapted to the rapid geopolitical and technological changes it is being confronted with.

This December 6, 2023 roundtable event was held to discuss root causes of the inertia inhibiting transformation, identify key obstacles, and generate insights on potential solutions. Subject matter experts from a variety of backgrounds across industry, government, academia, and the CAF discussed digital transformation as a culture and mindset challenge across new and old ways of doing business; operational and institutional considerations and the imperative of interoperability; untapped entrepreneurial potential within and outside the CAF; the political environment and legislative challenges; and how emerging technologies are being fielded today and what potential they hold for tomorrow.

This report provides a detailed analysis of the critical role of the digital transformation in sustaining Canada's defence capabilities and equipping it for the future. It underscores that while digital transformation is a far-reaching challenge, continuing to delay will have significant consequences for Canada's security and defence in terms of diminished capabilities and standing among allies.

Navigating the Digital Domain: Challenges and Opportunities for Defence

Military operations rely upon how fast one can create a clear picture with the information available, make a decision, and act on it. Digital and emerging technologies are accelerating that decision loop. Canada lacks a continuous deployment pipeline for software systems and currently has a one-year cycle to update its land C4ISR system, creating operational risk as Canada will predictably be behind allies and partners.

To enable digital transformation, the following ingredients are essential:

- unity of understanding,
- unity of purpose,
- experimentation, and
- executive sponsorship.

Unity of understanding and unity of purpose are achieved when different ways of looking at a problem converge to form a shared conceptualization. Experimentation is the iterative process by which pathways to a solution are identified and tested. Executive sponsorship is the prerequisite that enables the enterprise by providing the 'pull' from the top. In order to pull in the right direction then, it is critical that leaders know what to ask for and communicate that they are willing to be involved.

The following two examples outline how rapid transformation can be achieved when these criteria are met.

Digitally Aided Close Air Support (DACAS), 2017

In the late 2010s, the United States Air Force (USAF) sent a letter to all NATO nations advising that USAF was upgrading the process to request and coordinate Close Air Support, from voice to a fully digital ecosystem. By the early 2020s, if nations wanted to retain the option for their ground troops to call for USAF Close Air Support, they needed to acquire a compatible digital solution. The letter created urgency in the Canadian Army as USAF is the biggest provider of fire support and all ordinance requests had been conducted via radio up to that point. The impact of the letter on senior leadership was significant, as was its ability to fast-track a project through Canada's perpetually stagnant procurement system: while the DACAS initiative represented a relatively small project, it absorbed disproportional attention. A clear problem with tangible consequences provided unity of understanding and purpose and injected the project with a sense of urgency. Eighteen months after identification, the capability was in the hands of soldiers.

NATO Federated Mission Networking (FMN), 2021

In 2021, due to COVID restrictions, the signal regiment responsible for the CAF's interoperability with allies was not able to travel to Europe for the NATO FMN exercise, which is the exercise that ensures all participating allies' C2 systems can communicate with one another. With a timeline of six months to prepare, the regiment made it work, which prompted a visit by the Chief of Combat Systems Integration (CCSI) and several generals.

It is critical that there be a collective determination on priorities and objectives the CAF should pursue. Once those are established, the respective roles of industry, government, and serving and retired military will come into view. The present constraints are largely derived from the fact that clarity of consensus around what the CAF should hope to achieve is lacking. By contrast, the Americans have identified joint domain awareness as their top priority, which serves as the driving force behind efforts to modernize their forces.

There is need to foster more synergy among the S&T community, industry, startups and the military. The present system was made to tightly control communications between industry and government to ensure fairness, but it ends up costing the government in terms of outcomes by greatly constraining what can be said and achieved. Having an open forum is key to alleviating bottlenecks.

This brings another question to the fore, of whether there is sufficient space being created outside bureaucratic processes to allow for the development of intellectual curiosity and learning. The technology changes rapidly, and at an increasing clip, but if the people requesting it, or using its precursors, do not understand it or how to gain practical access to it, then they will not feel empowered. A kind of learned helplessness set in – the opposite of innovation.

Once meaningful progress can be made on enabling technology rapidly, there will be a groundswell of ideas. That is true for all of government and needs to happen across all departments. The digital piece is tied to the culture piece.

Operational and Institutional Perspectives

The Chief of Combat Systems Integration (CCSI) is responsible for enabling the CAF's digital transformation. It advocates for joint capabilities informed by allies and ensures the CAF remains credible through interoperability of command and control (C2). The expectation to keep abreast of allies is clear. While Canada's allies have been as accommodating as they are able, they will ultimately not wait on Canada as the pace of the threat precludes that choice. It is therefore critical that Canada demonstrate meaningful progress, or it will not be able to bridge the growing gap.

The development of a national cloud-based C2 solution that ties into the FVEY (Five Eyes) system is central in this respect. Three of Canada's FVEY partners are modernizing their C2 concepts. The CAF's version is the pan-domain concept, which has central to it the importance of FVEY interoperability. The US has been operated a series of quarterly exercises throughout 2024, which will frame interoperability requirements through which FVEYs will have to crew, train and equip their forces to ensure interoperability by 2025. Though the tight timelines dictated by allies magnify challenges inherent to solving its cloud interoperability problem, the CAF must make progress in order to achieve its limited interoperability goals by 2025.

The requirement to maintain interoperability for operational credibility cannot be understated. In this respect, Canada does not have a technology deficit; it has a policy and process deficit that impedes its ability to remain technologically current. There are no alternatives to the fact that the future of C2 is cloud-based, yet Canada is still operating on industrial age procurement policies that hinder cloud adoption while the United Kingdom and Australia will be joining the US in a secret cloud in 2025.

The three critical elements for success are:

- data-centric security,
- zero trust, and
- Identity Credentials Access Management (ICAM).

If zero trust is not achieved, then the CAF cannot be a viable partner or ally. It will take some years to get there, but it if pursued in a focused manner driven by training objectives, the CAF will be able to achieve a limited degree of interoperability with FVEY by 2025.

Determining aims and requirements

DND established the first digital transformation ADM (Assistant Deputy Minister) in the department, purposed with seeking new ways to do the business of defence. The most difficult part of the equation is determining what DND, and the CAF wants to achieve and where they want to be. The biggest requirement for the CAF to achieve its needs revolves around data flow, data quality, and data governance. Data is an existential asset for Canada's future, but where the Government of Canada has failed in its approach to data is attempting to do too much at once. The focus should be on open, shareable, and high-quality data.

The challenge that is encountered with Defence Research and Development Canda (DRDC) is how to move from development to use case and to implementation.

There are currently silos of expertise with respect to the handling of intelligence mission data and there is no homogenous understanding of how 'open' data ought to be or where it ought to reside. Work is being done to set up the needed data standards framework to achieve credibility and interoperability, and ultimately to enable better decisions faster. Necessary to the functionality of the framework is to establish a clear line across mission planning and mission execution. This is an example where industry expertise and capacity could be leveraged to accelerate data-enabling efforts.

Interoperability implies a choice of alignment, which creates access. To decide to be interoperable is to choose to align with certain policies; however, conferred access does not come free and will not last indefinitely. There is willingness among Canada's allies to share access right now, and Canada must respond with demonstrated willingness and commitment. Some of Canada's allies have already solved the data standards issue, and where it makes sense to adopt wholesale those standards, that should be considered. If Canada does not take the commitment to interoperability seriously today, including the concomitant effort to remain abreast from a policy and technology points of view, then access will eventually be curtailed or denied (as in the example of close air support).

The Canadian defence ecosystem

The larger defence ecosystem is not currently adept at taking R&D and turning it into a sellable product that solves a specific problem. Because R&D operates more or less in a controlled environment, the immediate output of R&D activities does not result in sellable products but rather in concepts. While R&D is a crucial step, more attention needs to be paid to productizing these works to get products in the hands of operators. In this respect, there is a need for more in-between sales opportunities for startups and small businesses to achieve product-market fit and deliver a competitive advantage. Given sales to a company's government are generally key to successful international marketing of military capabilities (e.g. folks will not buy 'it' if their government is not a customer), there will be limited market potential if there is no market inside Canada. The Canada and the CAF therefore have a role to play in creating demand for solutions from industry, which in turn will stimulate industry research, development, and production, ultimately enhancing readiness.

In order to achieve greater calibration between the CAF and the defence industry, Canada must develop its long-term strategy outside the narrow focus of catching up with allies. When factoring in estimates that Canada is 7–10 years behind allies, to focus its strategy solely on catching up will likely keep Canada perpetually behind. Canada must therefore determine a long-term strategy to grow its domestic defence industry informed by its own needs and capacity.

Technological trade-offs

While senior CAF members have expressed receptiveness to AI (artificial intelligence) investments, when the decision comes down to equipping troops with their most basic requirements or investing in capabilities to keep abreast with global advancements, the former is non-optional. Entrepreneurs and tech talent in Canada represent some of the best across the globe, but there is little business incentive to work with the CAF or in defence as they are not an easy or fast buyer to work with.

When the CAF does not have what it needs, there should be opportunity for startups to provide for those needs at the tactical edge to help soldiers with their most basic tasks. Technology needs to be pushed to the edge so engineers can hear directly from soldiers what their needs are, and being under contract from the armed forces is the only way to get the product into the hands of operators to receive constructive feedback and refine the product accordingly.

In-between sales generate the cashflow necessary for a startup or small business to scale, which opens up opportunities with Prime Contractors, System Integrators, and Original Equipment Manufacturers (OEMs) and provides a path by which their products can be integrated into enterprise-level capability offerings in Canada and in foreign markets. Startups need a clear and proven path-to-sale.

There is buzz around emerging technologies, but the reality is that many of the problems facing the forces today can be solved without them. The CAF has relatively limited fiscal and implementation capacity, and thus cannot do it all. Key decisions and trade-offs between operational staples (e.g. radios) and emerging technologies (e.g. AI) will need to continue to be made so it is incumbent to understand where it makes operational and fiscal sense to employ emerging technologies and where it is not necessary. That is not to say investments into emerging technologies are of secondary concern, but that investments need to be targeted.

The Canadian Political Environment

Is Canada seized of the issues?

As advances in emerging technologies are being exploited in the military context to gain decision advantage over adversaries in operational domains, these technologies are also being exploited by authoritarian governments and other threat actors in the political and civilian contexts to entrench anti-democratic values and policies.

Neither the Canadian government nor Canadian society has fully absorbed the full spectrum of risks and benefits involved with an increasingly digital world. From a political standpoint, we are far behind on the ethics and privacy standards in dealing with AI, facial recognition, and racial profiling, and how it is being used against citizens and by state and non-state actors against Canada and its institutions. From a cyber standpoint, while there is confidence in the cloud, it is not clear whether enough data has been moved to the cloud to better prepare and defend against a cyber-attack.

Interests and incentives

Beyond the legislative processes and regulatory frameworks that need to be updated, a question arises whether parliament has the necessary knowledge or capacity to deal with digital transformation, or if not, a plan to develop the capacity.

The primary responsibility of government is to ensure the security of Canadians, and that must start with national defence and homeland security. There is an existential nature to the security of our times, yet it is a relatively small proportion of parliament that is interested in defence and security. There are problems related to interests, incentives, and consistency, and these problems are particularly pronounced in government because people are constantly moved around.

MPs do not earn votes based on defence and security. There might be three or four ridings in all of Canada that actually care about security and defence and could shift the vote. Constituents' interests are to some degree shaped by what their MP communicates.

Novel threats and archaic systems

Digital transformation is pretty easily understood by people who want to protect themselves. Defence is a given, but to what extent is it equally important that Canada develop offensive cyber capabilities in support of national security interests? The conduct of offensive cyber activities is fundamentally different when conducted outside or inside Canada. Canadian and international laws, Canadian statutory authorities, and Crown Prerogative all play key factors in establishing functional parameters. The risk of foreign interference from actors including China, Russia, Iran, India and others is a significant threat, one which requires a both proactive and reactive response measures. Moreover, novel threats such as China setting up police stations, infiltrating universities, and influencing our political system calls for cogent and deliberate approaches that are more than reactionary.

Improved models for legislative access

There is thinking that needs to go into what could be changed with regard to how MPs interact with constituents so that Canadians have access to officials and to information that is not so artificially scripted. More MPs need the security clearance and should be provided more current, relevant information and intelligence.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) model has merit. Members are sworn in and given information, though despite its name it is not a parliamentary committee—it reports to the Office of the Prime Minister (PMO). It would be more effective if the defence committee could operate at a higher level of security as well and remain a stable committee rather than getting shuffled according to the leadership of the day.

In the Canadian system, unless an individual is appointed as a minister, they do not receive a security clearance. Canada's American colleagues provide a point of comparison here—if an individual is on the national security committee, they automatically acquire top security clearance and they are privy to information with which they can make impactful decisions on defence and security. The British also have a select committee on defence, and being that Canada is in the New Westminster system as well, the Canadian government could do well to learn from the UK Government example. One solution that the Canadian government could implement to improve information access and decision-making ability would be for MPs to undergo an application and screening process for top security clearance.

The Digital Frontier: Emerging Technologies in Defence

Cloud technology as the digital backbone

Two themes that arise in discussions on emerging technologies in defence are operational intelligence and the industrial metaverse, or 'meta-reality.' Cloud technology and its related capabilities are poised to have a significant impact on military organizations and the defence industrial base. When deployed appropriately, these technologies can drastically improve outcomes and processes in defence and intelligence.

The cloud can be grouped into three broad categories: the public cloud (or hyperscale cloud), the private cloud (such as those managed by governments), and edge capabilities (devices that can run connected or disconnected to a main cloud). The hyperscale cloud is considered essential for secure, high-power computing capability, and is crucial in the application of large AI models and the industrial metaverse.

Defence organizations want the following components in their digital backbone:

1. A scalable and efficient computing infrastructure capable of delivering hyperscale cloud.

2. Data connectivity across all operating domains.

3. The ability to make data-driven decisions at the tactical edge when necessary.

4. A robust cybersecurity foundation to protect the digital backbone.

The US has invested in the backbone—that is, C4ISR—in both the public and private cloud more than anyone else can. The ability to project power and provide a cloud-based backbone using space connectivity has already been proven by the Ukrainians. Within months of Russia's invasion, Ukraine transferred all their datasets into the public cloud using the US-based Starlink, which enabled them to stay in the fight through leveraging cloud infrastructure and 5G for targeting, fire control, C2, and intelligence operations.

Under standard operating conditions, the tactical edge is connected to headquarters and edge data can flow into the cloud datacentre to inform situational awareness, analysis, and further instructions. However, in DDIL (denied, disconnected, intermittent and limited) bandwidth environments this connection may be compromised, and the tactical warfighting unit would then need to process and interpret the local data themselves. In such a scenario, the sheer volume of data necessary to compute to make an informed decision would require cloud capabilities at the edge.

Any dependency on digital infrastructure naturally invites attention from the enemy to attack it, thereby increasing the threat surface area in the digital domain. Many analysts have observed that the greatest vulnerability in the digital backbone is network security. Unpatched and unmanaged devices presently represent a significant threat to network security, underscoring the need for greater awareness of digital hygiene and best practices as a baseline requirement. At the strategic level, the greatest weakness for Canada is its ability to force multiply, highlighting the need for cloud capabilities to manage the sheer volume of data involved in modern operations.

Personnel and facilities

In the military workplace, emerging technologies like enterprise resource planning (ERP) systems, internet of things (IoT), and augmented reality all provide real time insights and expertise to inform and guide personnel actions whether on deployment or in garrison. IoT Hubs are being deployed to monitor platform locations, headings, displacement and performance. This is familiar territory with air platforms, but innovative approaches such as those of the US Army Corps of Engineers, who have successfully automated dredging vessel activity, are instructive.

The capability lifecycle

Emerging technologies enable defence departments, the Armed Forces, and the DIB to effectively collaborate across the entire capability life cycle. The adoption of systems like digital engineering allows for rapid progression from a concept to a digital rendering of the platform, to then building it out and running it through mission scenarios. These intelligent modeling and simulation scenarios employ digital twins to deepen conceptual understanding of requirements, accelerate the design process, and ultimately improve maintenance outcomes. Digital twins are currently being used extensively by OEMs on the Canadian Surface Combatant and in the British Future Combat Air Program.

Combining intelligent modeling with predictive analytics and AR/VR (augmented reality/virtual reality) enables computers to analyze schematics to pull something out and determine when it was last replaced, what is required to maintain it, where to acquire the replacement and even submit the request for replacement. Other means that would support Continuous Capability Sustainment include 3D printing and software-based capability updates. When combined with the power of generative AI, prescriptive analytics and robotic process automation, sustainment activities across the defence enterprise and on operations will be significantly improved.

Optimize Design Advantage

Challenges to C2 and operational planning lie in the manual processes that impact decision speed, the varied maturity of AI/ML (machine learning) understanding and availability, and the handling of large amounts of unstructured, classified data necessary to operate in hostile environments. AI and cloud technology can enhance C2, modernize the intelligence cycle, optimize mission planning and execution, and automate mission readiness.

AI can handle large amounts of data and allows the human in the loop to optimize decision-making. Integrated Visual Augmentation System enhances soldiers' situational awareness with features like 3D terrain maps. DIB Independent Software Vendors leverage cloud platforms and AI to provide readiness assessment and optimization solutions at enterprise, operational, and tactical levels, which enables faster observation and decisions. This capability has already been fielded on ships, enabling sailors to resolve issues by connecting with a remote expert to guide them so they do not have to go into port.

Enhance interoperability

Tactical interoperability challenges among NATO allies when orchestrating combined and joint missions include C2 and technological disparities, doctrinal differences, and resource gaps. With respect to C4ISR interoperability, challenges include the limited ability for coalition classified information sharing, cross-agency info sharing, cross-industry collaboration, and the high volume of data and fragmented data sources. Given that data underpins virtually all of these challenges, expanding multinational and interagency collaboration through trusted and secure data sharing is critical. Inconsistencies between intended and actual operations of major defence systems are issues that require better DIB (Defence Industrial Base) integration. American data should be able to arrive in a Canadian data centre—this is already doable through independent software developers and available through the cloud.

The modernization of the defence IT stack is the other side of this coin. Commercially available SaaS solutions for productivity and collaboration are being deployed by militaries from the Unclassified to the Secret and Top-Secret levels. These solutions are addressing technical debt, improving security and greatly enhancing the user experience when compared with legacy C2 and operational planning tools. Integration with AI copilots is one example that significantly enhances situational awareness and improves productivity across the enterprise and the Armed Forces both in garrison and on deployment. PaaS and SaaS solutions allow developers to rapidly produce applications that leverage ground up innovation in response to challenges experienced by war fighters and administrators every day in the field.

The cloud project environment

The government must advance policy to knock down regulatory barriers, where appropriate, to make it possible to build cloud environments for clients. The Ukrainian experience provides some direction here—citizens have helped to develop management systems and deploy them to the armed forces because they have access to all the necessary tools.

The public cloud is so powerful because of the cyber solutions that run on it. About 99% of cyberattacks happen on private clouds because they are not monitored and updated as needed. This could be drastically reduced with basic digital hygiene. DND does not have the capacity to keep up with defending against so many attacks alone, but large corporations like Amazon, Google and Microsoft do.

There is great benefit to the hyperscale and having multiple redundant links. Though redundancy creates multiple points of failure and vulnerability, it also increases resiliency and the chance of survival. In this regard, we can look to Ukraine once again. If Russia wants to attack the data the Ukrainians are using, they would have to declare war on a third country to do so. That is precisely why you have edge devices with data centres spread across multiple regions.

At the national level, it became necessary for Ukraine to run their data elsewhere. While this involves greater vulnerability, it is more likely to survive. Ukraine proactively began moving their data out of their data centres and into the cloud, and they continue to operate as a government because of that. Cloud technology provides greater ability to isolate an attack and limit damage. Due to the scale of the cloud alone, distributed denial of service attacks are not feasible for an adversary. If Microsoft's cloud goes down, every corporation in the world goes down, in every government.

Know what you want

The procurement team is going through the motions, but they are not asking for the right things, and they are not considering what the current cloud offers. To stand up a cloud, the greatest hurdle can often be found in the contracting paradigm. Even with compatible technology, if the contract differs, it will not work. If F-35s are going to be connected, the proper authorities need to be in place to be able to connect them to the cloud services in order to use the technology.

There are policy constraints relating to sovereignty with respect to what data can be shared when combining the hybrid cloud environment with edge capability. Although safeguarding data sovereignty is enshrined in policy, it is ineffective in practice as Canadian data is already in Russia, China and elsewhere, which begs the question why these policies do not reflect the reality.

There must be a viable business case for transforming the way the institution currently works. Yet, there is still not enough literacy at the command level. Commanders need to own the subject and understand it to determine priorities. In many cases, there are veterans with a wealth of experience that can be exploited. However, there is an ingrained mindset of not trusting veterans once they are out—this gap must be bridged in order to take advantage of the experience and knowledge capital they offer.

Conclusion

Digital transformation is not merely about transitioning processes and protocols from one system to another, it is a complete transformation of the way of doing business in order to address new challenges that Canada and the Canadian Armed Forces are being confronted with in an increasingly unstable world. This requires concerted collaboration across DND and the CAF and with industry and external stakeholders. In order for any collaboration to bear fruit, there must be a shared understanding of the issues and stakes across the wider Government of Canada, particularly with key departments involved in procurement, and actions taken to address archaic policies and overcome inertia.

At the political level, much works remains to break defence issues out of partisan divides. In this regard, it is incumbent upon politicians to recognize the consequences for Canadians should the CAF fall further behind allies in its efforts to digitally transform. If Canada's forces are not interoperable with those of its allies, it jeopardizes Canada's ability to contribute to allied objectives, and inevitably raises the question of whether Canada will be able to offer the relevant capability when required, affecting our standing as a reliable Ally and Partner.

Acknowledgements

The CDA Institute thanks the Department of Defence MINDS program for supporting this event, as well as the speakers for sharing their expertise and insights as summarized in this report, and all participants who contributed to the discussions.