CANADIAN
ARMY ✠ **ARMÉE**
CANADIENNE

MODERNIZATION VITAL GROUND:
DIGITAL STRATEGY
The Essential Digital Pivot to be Effective in the Pan-Domain Fight

DIGITALLY ARMED
TO PROTECT
OUR TOMORROW

National Defence   Défense nationale

Canada

MODERNIZATION VITAL GROUND:

DIGITAL STRATEGY

The ***Essential Digital Pivot*** to be effective
in the pan-domain fight

STRONG. PROUD. READY.
FORTS. FIERS. PRÊTS.

CONTENTS

COMMANDER'S VISION FOR TRANSFORMATION

1. When we published *Advancing with Purpose: The Canadian Army Modernization Strategy* (CAMS) just over a year ago, our former commander — now Chief of the Defence Staff, General Wayne Eyre — said in his introductory remarks that "the Army we have is not the Army we need" to succeed in the emerging joint, pan-domain fight. As we have aggressively pursued the necessary change agenda prescribed in CAMS, and the "army we need" has progressively come into focus, it's increasingly evident that Digital Transformation is foundational to almost every aspect of this modernization. Frankly, I believe that without a significant *digital pivot*, the Canadian Army (CA) will fall short.

2. With this realization, it is clear that our previous relegation of Digital Transformation to 1 of 20 "nested initiatives" within CAMS *insufficiently emphasized the criticality* of Digital Transformation to our modernization program. Digital Transformation is of such importance to all aspects of CAMS that just like the Combat Team is the Vital Ground for CA training, Digital Transformation merits the title of **Vital Ground to CA Modernization**, and with it, its own strategy: parallel, complementary, and foundational to CAMS.

3. One thing is clear: Digital Transformation is not about transforming our current digital things into better digital things. It is about changing our entire relationship with technology, bringing the CA from an analog organization with legacy industrial-era force structures, tools, processes, governance models and culture, to a true, data-driven, innovative organization that maximally leverages the military potential of digital solutions to influence the battle in our favour — both in the office and in the field.
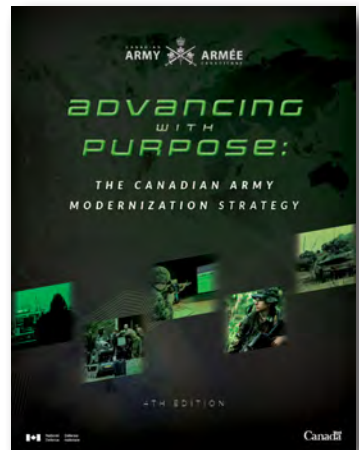
4. The modern battlefield is increasingly sensor saturated, with integrated, interoperable information systems and networks providing the backbone of our contemporary warfighting capability. Indeed, there is very little that we do that isn't enabled or mediated by technology; from how you are currently reading these words, to how a Forward Air Controller requests Close Air Support using an app in the middle of a firefight, to how we prepare financial forecasts to inform procurement decisions. And we need to get much better.

5. Our allies and adversaries increasingly integrate advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) into their institutional and operational processes to optimize existing capabilities, enable timely data-driven decision-making, and generate new capabilities while economizing the human cognitive workload for reinvestment into higher-value pursuits. Through large-scale digital integration and experimentation, they have already demonstrated that for closing the sensor-to-effector loop, current methods at their best are no match for AI-enabled fires. I believe that tomorrow's military history books will describe Digital Transformation as one of the great military advances, in the same category as the invention of the machine gun, mechanization, or the telegraph — it will revolutionize the way we fight.

6. Innovations in technology are accelerating and converging to create novel capabilities that we can only leverage by transforming our relationship with this technology into something more symbiotic. This strategy document is meant to lay the groundwork for the strategic level engagements and decisions required to publish an implementation plan aligned with the CAF's forthcoming Digital Campaign Plan. We need to tackle this urgently, and I solicit your engagement as we move this foundational discussion forward to seize our Modernization's **Vital Ground**.

SEARS – DIGITAL BANKRUPTCY

IN 1969 SEARS WAS THE LARGEST RETAILER IN THE WORLD. Sales from Sears represented 1% of the entire United States economy. Two-thirds of the population shopped there. In 2005, they were a 55 billion dollar company, yet in 2018 they filed for bankruptcy following two decades of financial hardship stemming from declining sales. Many believe Sears failed because the company was unwilling to innovate, but innovation was a significant component of their business identity. They were pioneers of the retail industry; Sears was the first to see railways as an opportunity to reach a broader customer base, they invented the mail-order catalogue, and deployed the first store-owned credit card with massive success. With a rich history in innovation, it was, in fact, Sears' governance that led to its downfall. The company's organizational structure was highly divisional, which saw a series of executives for over 30 departments (tires, appliances, apparel, etc.), essentially operating as standalone companies that competed against one another for funding and projects. While this allowed them to scale rapidly, their governance model was not suited to accommodate the growing technology trend and their inability to adapt made digital transformation impossible. Instead of a consolidated, centralized, digital business environment, the company supported different digital ecosystems for each division, with no over-arching architecture, alignment, or strategy. What resulted was a competitive, disparate digital infrastructure with a mass duplication of systems and needless investments across the business. COSTS AND INEFFICIENCIES RAN RAMPANT WITH SEARS' UNWILLINGNESS TO ADOPT A CONSOLIDATED DIGITAL APPROACH.

LESSON: DIGITAL IS NOT A PANACEA; IF NOT DONE RIGHT, IT CAN GO VERY WRONG.

DIGITAL LEGO BLOCKS?

WHAT COULD BE LESS DIGITAL THAN A SET OF LEGO BLOCKS? In 2003, old-school, analog LEGO was on the brink of bankruptcy. Company executives needed to find a different approach and finally prioritized digital transformation above all else — the company's corporate strategy and its digital strategy became one and the same. LEGO has been thriving ever since, investing a considerable sum of money in mobile games, mobile applications, and movies, blending the physical and digital worlds, and have experimented with 3D printing, allowing customers to create their own products. Additionally, the company is continuously working on research and development, adding sensors and other sophisticated elements to their blocks to cater to digitally-savvy customers. They even have an AI-powered application using visual recognition to translate pictures into LEGO models, and another app to teach children how to code. LEGO IS A COMPLETELY REIMAGINED, DIGITALLY TRANSFORMED COMPANY, AND THROUGH THIS PROCESS HAS RESTORED ITS STANDING AS ONE OF THE WORLD'S MOST VALUABLE BRANDS.

LESSON: LEADERSHIP "SKIN IN THE GAME" IS ESSENTIAL TO A WELL-EXECUTED, SUCCESSFUL DIGITAL TRANSFORMATION.

WHAT IS DIGITAL TRANSFORMATION?

7.   Digital transformation is best described as a wholesale makeover that occurs when an organization commits to forging a new, *symbiotic* relationship between its business and technology, using one to accelerate the other in a cycle of perpetual innovation and renewal.
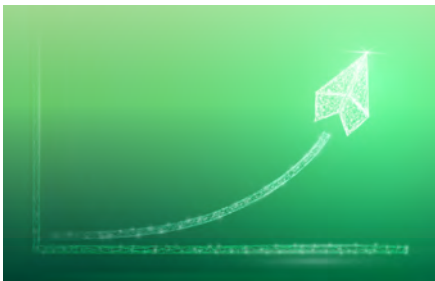
Digital Transformation is typically accomplished in a sequence going from initial ***Digitization*** to ***Digital Optimization*** to ***Digital Transformation***.

(As illustrated in the following table)

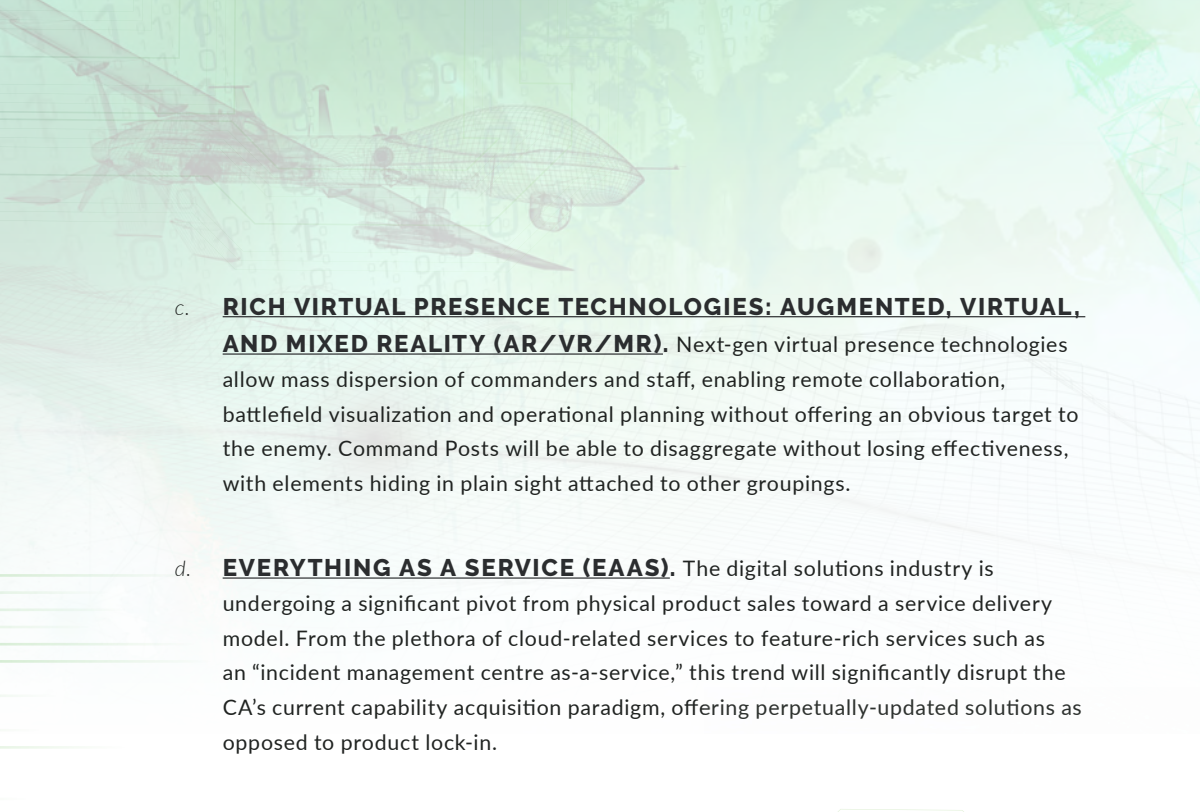| SEQUENCE	DESCRIPTION	EXAMPLE – OFFICE SPACE	EXAMPLE – BATTLE SPACE
DIGITIZATION	This foundational step refers to deliberately converting something non-digital into a digital representation or artifact.	Member completes their CF-100 Leave Pass on their computer, prints, signs, and delivers it to their supervisor for processing.	A software tool replaces a physical pin-board with a map, talc, and grease pencil to depict friendly and known enemy positions. The duty officer uses a keyboard and mouse to enter location data coming through the radio instead of a grease pencil. The COP has been digitized. Command Post (CP) staff are still doing the same job.
DIGITAL OPTIMIZATION	Once data is digitized, systems evolve to help consume and discover information more efficiently. Productivity and efficiency increase, improving an existing business process by supplementing human-driven actions without transforming them.	The same leave pass process is completed via Monitor Mass, enabling semi-automated filling of the data fields and allowing supervisors and administrators to process leave passes without hard copies of the documentation. The leave request process has not changed from the pre-digital era; it is the same workflow but entirely digitally optimized.	Modern software is added to the digitized COP along with robust tactical networks. This enables the automation of friendly force position reporting and enemy force position updates directly from sensor data and input on digital tools by forward-deployed friendly forces. This automated COP frees up the duty officer to focus on higher-order issues such as the evolution of the battle towards their commander's decision points and looking for opportunities to exploit. This sees no significant change to the roles and responsibilities of CP personnel.
DIGITAL TRANSFORMATION	Many organizations struggle to move beyond optimization. However, by forging a new, symbiotic relationship with technology, an organization can digitally transform, reinventing how objectives are accomplished and accelerating the entire business.	The CF-100 form is retired, and the responsibilities of administrative staff (regarding leave requests) are removed. When a member creates an event in their calendar and labels it as 'leave,' it automatically prompts their supervisor for approval. When approved, the system automatically alerts the member and reduces their remaining leave allocation.	The raw data from all available sensors in the area and the location, range, ordinances, availability, and time-to-effect of all effectors are continuously communicated to an AI algorithm. Upon detection of an enemy, the AI automatically identifies the target, picks and pre-queues the most appropriate effector and asks the relevant approval authority to engage, submitting along with this request a data-driven, collateral damage assessment informed by a machine learning algorithm that has assessed a library of past comparable engagements. The roles of personnel in the HQ are no longer the same; the organization has been digitally transformed.

DRIVERS FOR CHANGE

8.   **LAND WARFARE DRIVERS.** The idea that winning in the battlespace means one must win in the decision space is not new. What is new, is the exponential growth in the effort required to succeed in the decision space due to the sheer amount of data being generated by people and sensors, combined with the expansion and integration of potential military actions into new domains of warfare such as Cyber, Space and the Information environment. *The threshold to win in the decision space has simply moved beyond the processing capacity of humans alone and so technology must play an ever-increasing role in producing the decision advantage necessary to win.* Allies, partners, and our enemies constantly adapt their tactics, strategies, and digital technologies to accelerate commander decision-making thus increasing lethality. If we cannot interoperate with our allies through the exchange of raw data, we will restrict the power projection opportunities available to our government and will be unable to contribute to coalition support of national interests. The main Land Warfare Drivers include:

a.   **CHANGING CHARACTER OF CONFLICT (PAN-DOMAIN).** Conflict is no longer limited to the traditional domains of sea, land, air, and space. The cyber domain and the information environment are of increasing significance in influencing the outcome of a conflict, as can be seen in the Russian invasion of Ukraine. Pan-domain situational awareness will be critical to decision-making and only achievable through digital transformation.

b.   **RISK TO ENDURING INTEROPERABILITY AND RELEVANCE.** Our key allies are digitally transforming — and rapidly. Without a comparable effort on the part of the CA, our very relevance as a reliable ally will be compromised.

c.   **SENSOR SATURATION AND AUTOMATION.** Modern military tools, vehicles, resources, and weapons are not only becoming increasingly automated but additionally act as data harvesting platforms. We must create, retain, and exploit as much of this data as possible to achieve decision advantage on a dynamic battlefield.

9.   **INSTITUTIONAL ARMY DRIVERS:** The CA is expected to steward Canadian interests. While some digital tools have already been incorporated into management processes, further institutional drivers include:

a.   **OUTCOMES AND STEWARDSHIP.** Automating data collection, better data management, and new analytical and reporting tools will enable better decisions and reporting.

b.   **RECRUITING AND RETENTION.** New generations of soldiers are increasingly tech-savvy and enter the workforce having never known a pre-digital world. The CA is force-generating personnel with significant expectations of technological integration that can otherwise cause frustration and impact retention. Modern tools of a digital army must mirror real-world technologies in both intuition and function. This will enhance the digital soldier experience while decreasing the institutional learning curve.

c.   **POLICY.** Since 2017, numerous DND and CA policies and strategies have mandated the modernization of Defence business processes to better align with Government of Canada (GoC) expectations for digital services. Digitally transforming processes and capabilities will shape policy refinement, promising opportunities to optimize defence spending by enabling data-driven decision-making that will create efficiencies and improve the Force.

10. **TECHNOLOGICAL DRIVERS.** Technology is driven by the commercial market and accelerates at a pace the CA cannot match. We must seek to leverage the innovative solutions devised in the public sector, adapting them to our needs. Underpinning the warfighting and institutional environmental drivers are several complementary technologies that simultaneously reach maturity levels and declining costs favourable for integration. While not an exhaustive list, the resulting convergence of the technologies below, combined with too many others to list, will accelerate innovation, providing the CA with clear advantages if exploited, and potentially clearer disadvantages if not:

   a. **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (AI/ML).** Raw data of unprecedented volumes may only be processed into tangible information via human-machine teaming. Automating data exploration via AI/ML allows commanders to process more significant amounts of information while decreasing their cognitive load. This results in a decision advantage and an explosive increase in the speed and precision of warfare.

   b. **BIG DATA.** The digital world is founded by unprecedented amounts of data (referred to as 'Big Data'). This requires new procedures and processes to assure timely, reliable access to data — the foundation of a digital organization. As the battlefield becomes increasingly sensor saturated, the CA must exploit developments in communications equipment to increase data throughput and the rate at which it is processed (5G, Internet of Things, etc.).

c. **RICH VIRTUAL PRESENCE TECHNOLOGIES: AUGMENTED, VIRTUAL, AND MIXED REALITY (AR/VR/MR).** Next-gen virtual presence technologies allow mass dispersion of commanders and staff, enabling remote collaboration, battlefield visualization and operational planning without offering an obvious target to the enemy. Command Posts will be able to disaggregate without losing effectiveness, with elements hiding in plain sight attached to other groupings.

d. **EVERYTHING AS A SERVICE (EAAS).** The digital solutions industry is undergoing a significant pivot from physical product sales toward a service delivery model. From the plethora of cloud-related services to feature-rich services such as an "incident management centre as-a-service," this trend will significantly disrupt the CA's current capability acquisition paradigm, offering perpetually-updated solutions as opposed to product lock-in.

OBSTACLES TO CHANGE

11. The following items detail the obstacles to our success that must be addressed:

a. **DIGITAL CULTURE AND LITERACY:**
The foundations of a successful digital transformation are the right literacy and culture. Aside from a few "digital outposts" — innovators and early adopters within our ranks — as an institution, we have yet to embrace a digital culture, and many of us struggle to even recognize the delta between our current culture and the digital one we need — let alone realize why we might need it in the first place. This means that many of your would-be digital disruptors — full of ideas and ready to implement new tools that could radically improve our output — feel discouraged as opposed to empowered and enabled. This must change as a pre-condition for success. A digital culture is one where individuals and teams are encouraged to question the status-quo and re-evaluate, from first principles, everything they do and every problem they face with a *digital lens* — one that is grounded in digital literacy. They are emboldened to try new, digital ways of achieving outcomes and aren't afraid to experiment and "fail-forward" to eventually land on the optimal, transformative solution.

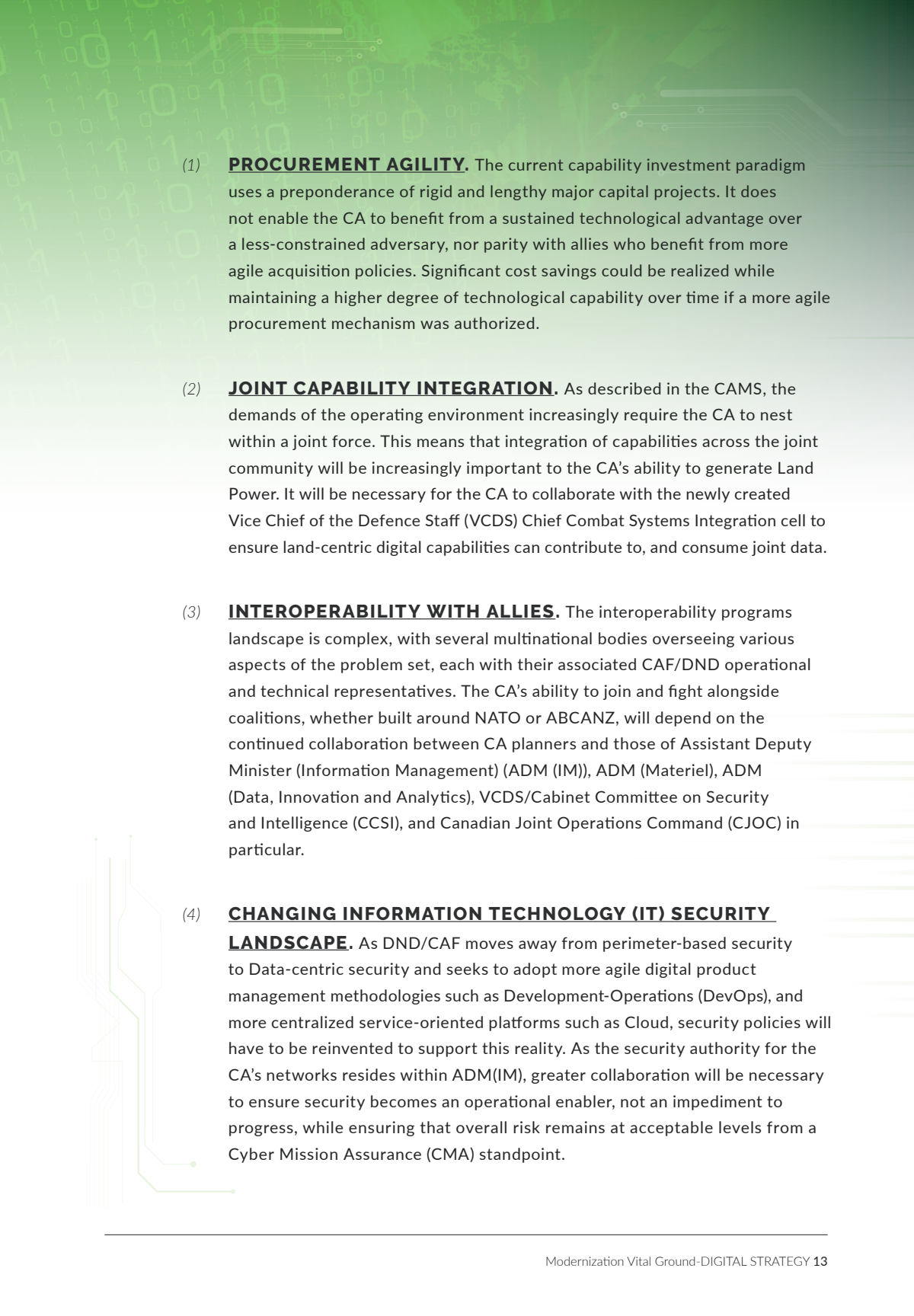b. **LACK OF DIGITAL LEADERSHIP AND INEFFICIENT DIGITAL CAPABILITY DEVELOPMENT.** Aside from culture, available literature on digital transformation, including lessons from allies, stresses the necessity of central, dedicated leadership from the very top of the organization. Success requires digital to become a tangible "C-Suite level" area of concern, with leadership "skin in the game." For this reason it is strongly recommended that the CA considers investing in a Digital Transformation Office, with its Chief Digital Officer (CDO) reporting directly to the Commander of Canadian Army (CCA) or the Deputy Commander of Canadian Army (DCCA) as a minimum, with appropriate authorities, accountabilities and responsibilities to speak both down/in and up/out on behalf of CCA. Without this leadership, the CA will not be able to sufficiently influence external stakeholders to enable this transformation, and internal initiatives risk misalignment with organizational priorities. Potentially worse, it could result in the acquisition of technical tools that are not exploited in a transformative way (same old methods using new tools) to reap the return on investment, thus risking the success of the entire exercise. Finally, our current industrial-age waterfall approach to capability development, applied to digital investments, is a serious obstacle to progress that will need influential key leader engagements across the department and GoC to address.

c. **LIMITATIONS OF CURRENT DIGITAL COMMUNITY OF PRACTICE (CAPACITY, FRAGMENTATION, AND TRUST).** A digital organization requires digital subject matter experts to become prominent advisors and leaders at all stages of operations to create, along with the process owner, the digital versions of the existing ways to achieve outcomes. The CA currently has too few experts. They are too fragmented to develop common approaches, and our current "digital winter" has eroded trust between operators and these experts. Cultural change and significant increases in resources for people, tooling and the capacity of our digital community of practice will be necessary to overcome these challenges.

d. **CAF/DND INSTITUTIONAL CHALLENGES.** The following obstacles to digital transformation are outside the CA's ability to address independently. That said, many are already captured in the draft CAF Digital Campaign Plan and the CA can play a key role in influencing the necessary changes to better enable our Digital Transformation:

(1) **PROCUREMENT AGILITY.** The current capability investment paradigm uses a preponderance of rigid and lengthy major capital projects. It does not enable the CA to benefit from a sustained technological advantage over a less-constrained adversary, nor parity with allies who benefit from more agile acquisition policies. Significant cost savings could be realized while maintaining a higher degree of technological capability over time if a more agile procurement mechanism was authorized.

(2) **JOINT CAPABILITY INTEGRATION.** As described in the CAMS, the demands of the operating environment increasingly require the CA to nest within a joint force. This means that integration of capabilities across the joint community will be increasingly important to the CA's ability to generate Land Power. It will be necessary for the CA to collaborate with the newly created Vice Chief of the Defence Staff (VCDS) Chief Combat Systems Integration cell to ensure land-centric digital capabilities can contribute to, and consume joint data.

(3) **INTEROPERABILITY WITH ALLIES.** The interoperability programs landscape is complex, with several multinational bodies overseeing various aspects of the problem set, each with their associated CAF/DND operational and technical representatives. The CA's ability to join and fight alongside coalitions, whether built around NATO or ABCANZ, will depend on the continued collaboration between CA planners and those of Assistant Deputy Minister (Information Management) (ADM (IM)), ADM (Materiel), ADM (Data, Innovation and Analytics), VCDS/Cabinet Committee on Security and Intelligence (CCSI), and Canadian Joint Operations Command (CJOC) in particular.

(4) **CHANGING INFORMATION TECHNOLOGY (IT) SECURITY LANDSCAPE.** As DND/CAF moves away from perimeter-based security to Data-centric security and seeks to adopt more agile digital product management methodologies such as Development-Operations (DevOps), and more centralized service-oriented platforms such as Cloud, security policies will have to be reinvented to support this reality. As the security authority for the CA's networks resides within ADM(IM), greater collaboration will be necessary to ensure security becomes an operational enabler, not an impediment to progress, while ensuring that overall risk remains at acceptable levels from a Cyber Mission Assurance (CMA) standpoint.

DESIRED STATE:
A DIGITALLY TRANSFORMED CA

12. As there is no "end" to digital transformation, this document will instead focus on illustrating what the *desired state* looks like. The CA will be digitally transformed when:

   a. decision-action cycles are revolutionized by new ways of processing, analyzing, presenting, and garnering insights from data, both in the battlespace and corporate space;

   b. at all levels, we see digital as a critical part of our armament ("digitally armed"), from which we harness our relative advantage ("...to protect our tomorrow");

   c. we have embraced a digital culture of experimentation, innovation, and perpetual renewal, with a new synergy between the science and technology, capability development, and operational communities — significant resources will need to be invested to fuel this necessary perpetual progress;

   d. we no longer see digital solutions as something static delivered by a capital project but as something we can build/optimize, at every level, as part of the solution to a tactical, operational, or institutional problem — we acquire agency over our digital tools;

   e. we have built a digital workforce, able to optimize and create new digital solutions, allowing us to *manoeuvre in the digital space*;

   f. integration with allies is a "fight tonight" capability baked into the design of all our digital systems; and

   g. we can integrate, synchronize and visualize our Land domain effects within a larger pan-domain context and meaningfully contribute to desired outcomes in other domains, including the information environment.

13. The desired end state is expressed as a series of *aim points* to guide the granular design of a future implementation plan:

a. **AIM POINT 1 — CULTURAL PIVOT TOWARDS DIGITAL INNOVATION.** We have embraced a digital culture of experimentation, innovation, and perpetual renewal.

b. **AIM POINT 2 — DIGITAL LEADERSHIP.** The CA has a Digital Leadership Office, reporting to CCA (or DCCA as a minimum), that effectively leads and manages all the activities necessary to digitally transform the CA. It is empowered to ensure the alignment of innovation and experimentation efforts across the CA enterprise, while also ensuring alignment with CAF/DND and wider GoC efforts in the Digital space.

c. **AIM POINT 3 — PARTICIPATIVE FORCE DEVELOPMENT.** Our processes for intake and development of digital solutions reach the lowest level, where the "analogue pain" is felt, thus providing unprecedented commander and operator agency over digital tooling.

d. **AIM POINT 4 — INTEGRATION OF TECHNOLOGY INTO DAY-TO-DAY BUSINESS PROCESSES.** The CA incrementally transforms warfighting and business processes, secured through cyber mission assurance, to accelerate outputs.

e. **AIM POINT 5 — INTEROPERABILITY.** The CA can exchange large amounts of raw data with allied nations in a tactical environment, to fuel machine-enabled analytics and computer-aided decision-making.

GETTING THERE:
FROM TODAY'S ARMY TO OUR DESIRED STATE

14. **LINE OF EFFORT (LOE) 1 — INVEST IN OUR PEOPLE.**
The CA's greatest asset is its people. They must be placed at the forefront of Digital Transformation by ensuring end-users are engaged and connected to the development of digital solutions. The CA must promote digital literacy across its ranks while reinforcing existing skillsets and recruiting new talent. This LOE includes:

   a.   increasing the digital literacy across all CA personnel;

   b.   recruiting and managing digital talent — including proactively amending existing job specifications to ensure training and equipment adequately reflect real-world expectations; and

   c.   embracing change driven by a digital workforce.

15. **LOE 2 — OPTIMIZE CA STRUCTURES AND TRANSFORM OUR PROCESSES.** Organizational, financial, and governance processes must evolve to keep pace with the rapid transformation incumbent upon a digital Force. Further, the CA must overcome our tendency toward process-based initiatives — we must remain mission-focused and remind ourselves that every action taken toward innovation should be directly related to delivering effects. This LOE includes:

   a. building digital leadership capacity in the CA;

   b. adopting a lean, agile governance model to keep pace with exponential digital growth. This framework exchanges big wins for small wins, which simultaneously suppresses the impact of losses;

   c. evolving our current project focus into a more integrated program and digital product management practice;

   d. reinforcing and expanding our military-industry partnerships to alleviate CA resource pressures (people, money, and time);

   e. integrating software engineers and developers alongside the end-user by adopting a DevOps framework; and

   f. gaining momentum toward transformational change via top-down encouragement of habitual experimentation. Leaders must defend against the 'Sunk Cost Fallacy' through a willingness to accept calculated risk and *fail forward*.

16. **LOE 3 — STRENGTHEN OUR RELATIONSHIP WITH DATA.** A Digital CA must view Data as the foundation for its ability to generate combat power. CA Data must be protected while providing reliable access in every operating environment — it is the fuel for digital systems. This LOE includes:

   a. empowering the Force to transform raw data into useful information via automated data analytics (AI/ML);

   b. adopting, implementing, and achieving industry standards and best-practices for data management to ensure quality and accessibility of data used in digital solutions and decision making;

c.   protecting CA operations by securing our data against the harshest digital adversary; and

d.   augmenting CA operations by assuring timely, global access to our own data and that of our allies.

17.   **LOE 4 — MODERNIZE OUR TECHNOLOGY.** Digital capability investments must be fully synergized between stakeholders and adopt a holistic, integrated program approach vice a project one. Digital initiatives will transform existing processes and workflows while retiring legacy systems. This assures force modernization without over-burdening technical support personnel with duplicate or parallel digital ecosystems. This LOE includes:

a.   integrating our current and future command and control systems into a unified network architecture;

b.   leveraging cloud computing;

c.   streamlining the end-user experience through device agnosticism;

d.   alleviating resources by outsourcing when possible, seeking everything as a service (EaaS) where applicable; and

e.   ensuring Force Development efforts adhere to an interoperable design.

CONCLUSION

18. ***IN THE DIGITAL AGE, AN ARMY THAT ENGAGES THREATS AT THE SPEED OF CHAT BOXES, POWERPOINT, AND VOICE COMMUNICATIONS WILL NOT EFFECTIVELY FIGHT ALONGSIDE, OR AGAINST, ONE THAT OPERATES WITH REAL-TIME COMPUTER-AUGMENTED TARGETING, PLANNING AND DECISION-MAKING.*** This document signals our commitment as an organization to forge a new relationship between our mission and technology — using one to accelerate the other. Together, we will accelerate CA efforts toward digital transformation; we will integrate all aspects of technology to enhance smart Land Power projection within an increasingly pan-domain fight. Achieving the desired state will be a significant undertaking, shaking the very foundation of the CA we have today. This may be a scary thought, but we have already established, in the words of our current Chief of the Defence Staff, that *"the Army we have is not the Army we need."* Therefore, we will necessarily and fundamentally alter the culture of the CA to one that embraces transformational change and deliberate risk acceptance to always *fail forward*. **We will transform how we conduct Land Warfare and run the Institutional Army, and through this transformation, ensure we are poised to win into the future in both our corporate spaces and tomorrow's battlefield.**

DRIVERS

LAND WARFARE

CHANGING CHARACTER OF CONFLICT *(PAN-DOMAIN)*	RISK TO ENDURING INTEROPERABILITY & RELEVANCE

SENSOR SATURATION & AUTOMATION

INSTITUTIONAL ARMY

OUTCOMES & STEWARDSHIP	RECRUITING & RETENTION

POLICY

TECHNOLOGY

ARTIFICIAL INTELLIGENCE & MACHINE LEARNING	EVERYTHING AS A SERVICE
RICH VIRTUAL PRESENCE TECHNOLOGIES	BIG DATA

LOE 1. INVEST IN OUR PEOPLE

LOE 2. OPTIMIZE CA STRUCTURES & TRANSFORM OUR PROCESSES

LOE 3. STRENGTHEN OUR RELATIONSHIP WITH DATA

LOE 4. MODERNIZE OUR TECHNOLOGY

OBSTACLES

LACK OF DIGITAL CULTURE & LITERACY

LACK OF DIGITAL LEADERSHIP & INEFFICIENT CAPABILITY DEVELOPMENT

LIMITATIONS OF CURRENT DIGITAL COMMUNITY OF PRACTICE

CAF/DND INSTITUTIONAL CHALLENGES

DESIRED STATE

AIM POINT 1
CULTURAL PIVOT TOWARDS DIGITAL INNOVATION

AIM POINT 2
DIGITAL LEADERSHIP

AIM POINT 3
PARTICIPATIVE FORCE DEVELOPMENT

AIM POINT 4
TECHNOLOGY-BUSINESS SYNERGY

AIM POINT 5
INTEROPERABILITY