National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DIGITAL TRANSFORMATION: HOW TO ENSURE THE CAF REMAINS A PARTNER OF CHOICE

Author: Anonymous

JCSP 49

Exercise Solo Flight

Disclaimer

PCEMI n° 49

Exercice Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

DIGITAL TRANSFORMATION: HOW TO ENSURE THE CAF REMAINS A PARTNER OF CHOICE

Author: Anonymous

DIGITAL TRANSFORMATION:
HOW TO ENSURE THE CAF REMAINS A PARTNER OF CHOICE

Digital transformation is now one of the world's newest megatrends[1] which has rapidly advanced since the Covid-19 pandemic. The defence sector is not immune to the swift impacts of digital globalisation and its subsequent threats to societal and state security, which can be driven by the weaponization of digital technology. Digital transformation will directly influence future society especially in respect to the global economy, communications, industry production and predictive monitoring of climate change activities[2]. As a global megatrend influencing both societies and states it will generate new demands on all sectors, cultures, and businesses. This in turn will challenge existing norms, creating shifts in perceptions and culture to likely effect the utilisation of digital transformation with both advantages and challenges to its global use.[3] With this will come both new expectations and threats to states, industry, and society. This will challenge security responses, including government, police, and industry. Defence, specifically the Canadian Armed Forces (CAF), must be able to exploit digital transformation to both project their military forces in equal partnership with their allies whilst preparing and predicting how their adversaries will exploit digital transformation to their advantage.

This paper will argue that without identification of current and existing digital transformation capability gaps, the CAF will fail to establish partnerships with global industries and their allies. The failure to do so will leave the CAF insufficiently prepared to respond to evolving interoperability, digital technology or personnel demands to effectively mitigate against future security challenges against Canada and put it at risk of self-relegating to the status of being a less than favourable coalition partner of choice.

This paper will first articulate a potential, but fictious, deployment scenario for the CAF to situate the reader on the expected likely demands for defence digital transformation response. Looking at the Government's approach, it will consider the Canadian Government digital transformation initiatives to understand the government wide demands placed upon the CAF. It will then assess the CAF's current response to approaching digital transformation and what challenges it will present by providing a summary of the digital transformation initiatives already in place by Canada's allies, including the United Kingdom (UK), Australia and North Atlantic Treaty Organisation (NATO). Throughout the paper, industry responses will also considered to highlight similarities or differences. Finally, there will be an identification of the benefits of digital

---

1 Michelle Scarborough, "4 Megatrends Shaping Post-Pandemic Digital Transformation," Business Development Bank of Canada," dated 2021, 4 megatrends shaping post-pandemic digital transformation | BDC.ca.

2 Hans Gillior, "Digital transformation: An Unstoppable Global Megatrend," Institute for Digital Transformation, dated 5th February 2018, Digital transformation – An Unstoppable Mega Trend (institutefordigitaltransformation.org).

3 Christine Agius, "Social Constructivism," Contemporary Security Studies, Sixth edition, Oxford University Press (2022).

transformation against the backdrop of the deployment scenario and it will articulate proposed concepts to better aid the CAF in addressing this current global megatrend.

Deployment Scenario for the CAF

The following scenario is used to frame the reader with an albeit fictious, but realistic scenario for a potential CAF deployment. This scenario will be used throughout the paper to align the reader with some of the well-known challenges that are presented to defence. Without investment, and a rapid approach to implementing digital transformation, these challenges will continue.

> Directed by the Canadian Government to support a kinetic response to an escalating conflict in Africa, the CAF is required to deploy a graduated response for its deployment of personnel and capability. Global Affairs Canada's (GAC) humanitarian relief has a footprint in location working as part of the United Nations (UN) mission. An initial CAF force of mobility aircraft and infantry soldiers is deployed to support humanitarian aid provision. Coordinating the CAF intelligence force with Canadian Security Intelligence Service (CSIS) to understand the posed security threats, the GAC diplomatic engagement within the country has so far led the negotiation activity with local government prior to the establishment of military forces. Monitoring of industry activity thought to be involved in the conflict, alongside movements of personnel and online commercial activity offer opportunity to build a data-rich picture with interlinkages, but activity so far remains unhampered. Multiple CAF units arrive in country, prioritising administration, and logistics staff due to complex manual processes with difficulties arising in the coordination of component capability generation due to limitations, planning timeframes and personnel information gathering delays. Within days of the CAF arriving in country, the internal conflict escalates, requiring a NATO led force to be deployed forward. Headquartered between Brussels and in-country, handover between the CAF and NATO is reliant upon physical handovers and sharing of information via sitreps or teleconferences. Rapid deployable communications systems have limited bandwidth due to the austere location, hindering the information flow to Canada, NATO, and in-country diplomatic teams. As the NATO forces deployment escalates, numerous nations arrive with incompatible security systems, planning processes and intelligence collection. Reliant upon satellite communications, due to the austere location, there is limited interoperability between the CAF systems, due to non-prioritised CAF investment in the NATO Federated Mission Network,[4] and a reliance upon unclassified systems to coordinate activity with other nations. Limitations on the number of personnel permitted to deploy by the Canadian Government are challenged by the Minister of National Defence, resulting in a reduction in the number of component capabilities, such as

---

[4] Department of National Defence, "CAF Digital Campaign Plan," Government of Canada website, dated 22nd February 2023, CAF_Digital_Campaign_Plan.pdf (canada.ca).

aircraft, to ensure there are sufficient personnel to operate safely due to the processes and limited data sharing between components.

Canadian Government Approach to Digital Transformation

Having identified a possible scenario for the operational demands of digital transformation in the CAF, this paper will now consider the Government of Canada's response to advancing its digital agenda in response to both domestic and international aspirations.

Canada proudly declares itself as a leading state in the implementation of digital transformation across Government departments. It has been driving the global change approach to digital transformation, which includes being a leading member of the Open Government Partnership with 75 nations, to realise action plans to incorporate multiple nations.[5] The Governments' 2022 digital ambition document is bold, setting tangible objectives for pan-Government departments, as well as providing comprehensive frameworks which closely replicate models used across industry and other nation's governments.[6] Although Canada has been serious about its digital transformation intent for several years, the CAF only released its first ever Digital Campaign Plan in 2022.[7] While the delayed response is unclear, it indicates either a possible disconnect between senior Government departments, a realisation in the time it takes to establish then implement a digital strategy, or perhaps the reality that the Department of National Defence poses more complex challenges compared to other government departments such as the Department of Transport. The Governments intent from the strategy is ambitious and addresses concerns such as infrastructure investment and an ability to generate digital literacy.[8] The Government strategy does not however identify any linkages between the advantages of digital transformation in addressing potential national security threats, missing an opportunity to emphasise the need for a pan-government digital strategy. This is in contrast with the UK's Government Digital Strategy, last released in 2022, which specifies national security is reliant upon, and instrumental to, the harmonious evolution of digital transformation and technology.[9] So, while the Government of Canada has invigorated its digital agenda, it has potentially missed an opportunity to starkly reiterate the importance of addressing security threats to its population using the common understanding of digital transformation to begin to mitigate these threats. The Government of Canada's agenda should thus offer the CAF an opportunity to use digital transformation to frame global trend security in an easily

---

5 Treasury Board of Canada Secretariat, "Digital Operations Strategy 2021 – 2024," Government of Canada website, dated 2021, Digital Operations Strategic Plan: 2021–2024 - Canada.ca.

6 Treasury Board of Canada Secretariat, "Digital Ambition 2022," Government of Canada website, dated 2022, Canada's Digital Ambition 2022 - Canada.ca.

7 Department of National Defence, "Canadian Armed Forces Digital Campaign Plan," Government of Canada website, dated January 2023, CAF_Digital_Campaign_Plan.pdf (canada.ca).

8 Treasury Board of Canada Secretariat, "Digital Ambition 2022."

9 UK Department of Digital, Culture, Media and Sport, "UK Digital Strategy," UK Government website, dated 04 October 2022, UK Digital Strategy - GOV.UK (www.gov.uk).

relatable manner for its population, whilst providing benefits to the delivery of its capability through advocation of digital literacy.

Digital transformation aspirations are not unique to governments or militaries. Arguably with a much earlier focus than governments, industry has embraced the global trends to digital transformation due to both the necessity to retain economic advantage, and the need to adapt to changing market conditions. Kravchenko describes the digital economy as "processes by which information technologies change economic and social relations in such a way that a number of barriers in international economic relations disappear altogether or minimize."[10] These could include opportunities to reduce costs, innovate availability of services or create new business opportunities enabled by digital transformation.[11] The industry digital transformation intent echoes that of the CAF's digital strategy "gaining a decision advantage over adversaries and maintaining interoperability with allies."[12] This statement identifies the parallels that exist between industry and government. Despite industry rapidly implementing digital objectives, there remains a huge lag in both the accountability and generation of international digital standards.[13] So, while from a state perspective Canada aspires to lead the international alignment, such as Open Government Partnership, it is at odds with the lived experience of industry in its implementation at home. It would be naïve of Canada to not learn from these observations, and it must ensure that in explaining its aspiration of improving digital transformation to its people and pan-government it is focused on interoperability, as opposed to aspiring to deliver solutions which replicate industry or exact international standards. This will be important in articulating the realistic key deliverables for the CAF strategy.

From a domestic angle, the Government's digital operations strategy articulates the expectation of the Canadian population to be able to 'access any government service, at any time, and on any device.'[14] Although not the CAF's sole responsibility to deliver, it does start to determine the digital expectation of serving defence members, but more importantly, those whom the CAF seeks to recruit. As Canada's population's digital skills improve, so will the expectation of the employer to both meet a perceived minimum baseline of digital services availability to employees. However, the CAF currently faces a steep initial challenge, with reports as recent as 2021 stating the CAF's IT systems were

---

[10] Olena Kravchenko, 'Digitalization as a Global Trend and Growth Factor of the Modern Economy," Bohdan Khmelnytsky National University of Cherkasy, Ceur Vol 2422, Dated May 2019, paper35.pdf (ceur-ws.org).

[11] Irina Aidrous, Ravil Asmyatullin and Sofya Glavina, "The Development of the Digital Economy: GCC Countries Experience," Industry Competitiveness: Digitalization, Management, and Integration, ISCI 2019, Lecture notes in Networks and Systems, Vol 280, Dated 15th August 2021, https://doi-org.cfc.idm.oclc.org/10.1007/978-3-030-80485-5_21 .

[12] Department of National Defence, "Canadian Armed Forces Digital Campaign Plan," Government of Canada website, dated January 2023, CAF_Digital_Campaign_Plan.pdf (canada.ca).

[13] Michel Girard, "Global Standards for Digital Corporation," Centre for International Governance Innovation, dated 28th October 2019, Global Standards for Digital Cooperation - Centre for International Governance Innovation (cigionline.org).

[14] Treasury Board of Canada Secretariat, "Digital Operations Strategy 2021 – 2024."

not sufficiently supported to match the demands of operations.[15] This is reported both domestically and on deployed operations and there are many areas to be prioritised and worked upon. Recognised in the CAF's Digital Campaign Plan, the CAF needs to ensure it grows digital literacy skills, rather than degrading them through operating on legacy systems and thus motivate employees to remain in the CAF.[16] Although this is a challenge to the CAF, it would generate high reward and benefits to the CAF overall.

Looking at the deployed digital scenario, with the Government driven approach to digital transformation already highlighted, this would set the momentum across the whole of Government. Harbouring opportunities for greater integration between departments, digital transformation would offer opportunity for improved data driven decisions, predictive data monitoring and would meet the Governments priority key deliverable for "getting value from the data."[17] For this deployed scenario, access to intelligence and coordination with pan-Government components such as CSIS or GAC could allow for greater collaborative working. It would provide greater confidence of information sharing and trust as well as a reduced forward footprint due to improved access to information to 'operate from anywhere concept'. However, this will require a collaborative vision between departments and pan-government oversight from the Minister of Digital Government[18] to both coordinate delivery of systems and services, but also to arbitrate the prioritisation of processes between departments.

Up until this point this paper has considered digital transformation from the Government of Canada perspective to identify how this will inform the CAF digital strategies, as well as the impact on the population and the CAF. It also considered digital transformation from the perspective of government and industry to determine the importance of partnership in addressing the digital transformation global trend challenges.

The CAF Approach to Digital Transformation

Taking forward the intent set by the Government of Canada for digital transformation, this paper will now consider how the CAF is approaching its aspirations to digitalise its workforce, operational outputs and identify potential challenges in the current CAF approach.

The CAF, and the defence environment in general, presents a complex set of challenges for digital transformation. Driven by a need to operate concurrently with different security classifications of information, integrating leading edge military capability, alongside demanding interoperability challenges with partners, there are very few other sectors who are presented with similar challenges. The CAF Digital Campaign

---

15 Lee Berthiaume, "Poor IT Support Hurting Canadian Military Operations, Internal Review Finds," Canadian Press Staff, dated 4th January 2021, Poor IT support hurting Canadian military operations, internal review finds | CTV News.

16 Department of National Defence, "CAF Digital Campaign Plan."

17 Treasury Board of Canada Secretariat, "Digital Operations Strategy 2021 – 2024."

18 Ibid.

Plan is the first formal step the CAF has taken in addressing this urgency with the Chief of Defence Staff (CDS) stating, "we shall not incorporate digital – we will become digital."[19] By way of comparison, the Raytheon Missiles and Defence digital transformation agenda emphasises the need to focus on digital and data to improve the speed of delivery; echoing the sentiments and parallels of both military and industry approaches to digital transformation.[20] The CAF's Digital Campaign plan however does carefully replicate the exact language used in all industry and government digital transformation strategies, especially sectors such as banking,[21] and it directs why the organisation needs to change to remain relevant while identifying specific programmes and key deliverables to enable success. The campaign plan is written in a relatable language for all of defence and is accessible online for industry, yet the terminology of 'digital' is rarely part of the military vocabulary. However, the CAF's Defence Policy, Strong Secure and Engaged (SSE) released in 2017, does not mention 'digital' at all, indicating a disconnect between the security threats identified in SSE and the campaign plan intent which may cause funding and prioritisation conflicts unless modernised.[22]

To address this apparent disconnect, the demands of digitalising the CAF will be heavily reliant upon both new technologies and ways of working across all elements.[23] This will require a change towards a digital culture, instead putting digital at the forefront of enabling defence management, processes, and capability for the CAF, rather than relegating it to simply a supporting element. This must also include digitising of processes, and thus generating efficiencies in areas such as a Human Resources (HR) workforce to allow reallocation of posts to other CAF capabilities.[24] The CAF will immediately benefit from this change, however digital transformation of a large organisation is not without risks. One research think-tank identified that both governments and industry businesses have on occasion failed to sufficiently protect their employers by taking digital transformation too far.[25] They have relied too heavily on digital transformation products and failed to provide human assurance checks which could mitigate against incorrect data prediction, discrimination, or misrepresentation. Although this has made some attempts to transform to a digital culture somewhat tainted, however the numerous benefits of digital transformation can far outweigh these concerns,

---

19 Department of National Defence, "CAF Digital Campaign Plan," p3.

20 Raytheon Missiles and Defence, "Digital Transformation," Raytheon website, last accessed 3rd May 2023, Digital Transformation | Raytheon Missiles & Defense (raytheonmissilesanddefense.com).

21 Steve Kent, "Digital Transformation: Digital Banking Strategies," Blog on CSI Web, dated 24th November 2021, Digital Transformation: Digital Banking Strategies Throughout the Customer Lifecycle | CSI (csiweb.com).

22 Department of National Defence, "Strong, Secure and Engaged," Government of Canada website, released in 2017, Strong, Secure, Engaged. Canada's Defence Policy.

23 Chris Nott and Richard Davies, "Digital Transformation in Defence – Balancing the Strategic and Tactical," IBM UK and Ireland website, dated 18th November 2021, Digital Transformation in Defence - Balancing the Strategic and the Tactical - IBM UK & Ireland - Blog.

24 Jennifer Buchanan, Beth Kelley and Alicia Hatch, "Digital Workplace and Culture: How Digital Technologies are Changing the Workforce and How Enterprise Can Adapt and Evolve," Deloitte website, dated 2016, us-cons-digital-workplace-and-culture.pdf (deloitte.com).

25 Chris Vallance, "TUC: Government Failing to Protect Workers from AI," BBC News website, dated 17th April 2023, TUC: Government failing to protect workers from AI - BBC News.

so long as mitigations are considered within the digital transformation strategy upfront. The CAF digital transformation programme must be a standalone capability, such that is recognised and understood by all personnel within the CAF, and crucially industry enablers, whom can all draw upon a central pool of information to ensure coherence and enable innovation in partnership from all aspects of the organisation and capability.

The CAF Vice-Chief of Defence Staff (VCDS) Digital Transformation Directive from December 2022 begins to address the requirements for the CAF.[26] Aimed primarily at the Level 1s (L1s) within the CAF, the directive specifies their expected outputs in support of digital transformation, placing the Government of Canada drivers to dictate the urgency. Although allocated $200m over five years for L1s to advance their digital responsibilities, digital transformation programmes are not inexpensive to implement, nor are the specialist contractor resources which are required to enable this ambitious change programme. Therefore, the Digital Transformative Directive may be at risk of non-delivery unless sufficient uplift in defence resources is prioritised to match the intent. It does however highlight concerns such as infrastructure enablement, routinely replicated in industry, where digital demands have accelerated quicker than the ability to provide supporting infrastructure or to improve digital literacy at a pace to match demand.[27] This is not a unique challenge to the CAF and thus it must be careful to not attribute excuses to the lack of resource in stopping it achieve its digital objectives; innovation aids this and industry has not been hindered.

As with the Digital Campaign Plan though, there is one constant missing from the Digital Transformative Directive: Industry. The CAF, as with the Government of Canada, within its strategies continually refuses to acknowledge the importance of industry partnership in enabling digital transformation. Engen's analysis against the CAF's approach to Artificial Intelligence (AI) strongly noted that digital transformation, and thus subsequent AI activity, cannot be achieved without strong partnership with industry and academia,[28] neither of which the CAF has openly invested any resources towards. Sadly, the Digital Transformative Directive and Digital Campaign Plan fail to identify streams of activity to bring industry into partnership with the CAF, with the directive stating that it's targeted to CAF employees' only. Without adjustment, this will not encourage industry partners to be engaged in programmes to jointly shape digital transformation initiatives for the CAF, or for industry to be tailoring their solution to

---

[26] Department of National Defense, "VCDS Directive for CAF Digital Transformation – Draft," Government of Canada document number 10711984, Version 27, dated 22 December 2022.

[27] Irina Aidrous, Ravil Asmyatullin and Sofya Glavina, "The Development of the Digital Economy: GCC Countries Experience," Industry Competitiveness: Digitalization, Management, and Integration, ISCI 2019, Lecture notes in Networks and Systems, Vol 280, Dated 15th August 2021, https://doi-org.cfc.idm.oclc.org/10.1007/978-3-030-80485-5_21 .

[28] Robert Engen, "When the Teeth Eat the Tai: A Review of Canada's Defence Artificial Intelligence," Defence AI Observatory, dated January 2023, DAIO_Study2309.pdf (defenseai.eu).

meet the exact demand from the CAF, both of which are core lessons learnt from digital implementation by industry. [29]

On the surface, the Digital Transformation Directive sets out clear strategic, HQ level intent for digital transformation objectives.[30] This includes the establishment of the Defence-X programme which will be leader led to improve operational effectiveness of the digital journey.[31] However, on closer inspection this activity seems to be limited to business processes only and does not address any of the CAF operational demands. As such, it is unclear who or when this will become a prioritised programme to support operations. More notably, the directive states that there will be up to $1bn invested over the next 10 years to deliver a 'digital led CAF by 2030' although the procurement Defence-X programme does not commence programme initiation, or allocation of funding, until at least 2025.[32] This is arguably a very ambitious target for the CAF, whom as a force remains heavily reliant on day-to-day paper processes which are dictated by higher level policy; all of which are processes that must be streamlined prior to digitising and moving forward to using digital for data prediction purposes and beyond. And while outside of scope of this paper, this is further compounded by the CAF procurement process which is not designed to support agile-technology growth,[33] requiring challenge to the processes from the most senior CAF level to meet these timeframes. The Defence-X programme is also reliant upon establishing governance offices by September 2023 as set out in the directive for digital transformation. Yet, with a currently inexperienced digital workforce, and a reluctance of the CAF to call upon industry partnerships and skillsets, the ability of the Digital Transformation Directive to gain meaningful momentum in the short term could be quickly diminished.

Reflecting upon the deployed digital scenario, by implementation and suitable funding of the CAF Digital Campaign Plan and Digital Transformation Directive, the CAF can begin to make significant changes at all levels of strategic, operational, and tactical business and operations. With a digitised and integrated with industry approach the monitoring of aspects such as logistics will allow the CAF to better predict and track movement of equipment, calling upon spares 'just-in-time' and reducing the forward footprint of equipment. The number of HR and logistics personnel would be dramatically reduced due to streamlined digital processes, allowing most of the support activity to instead be conducted from Canada or the NATO HQ. Capabilities such as aircraft support and personnel will no longer be restricted due to HR or logistics personnel taking precedence, and in parallel benefitting from improved equipment safety due to better data forecasting and improved links with industry. Finally, satisfying the Government of

---

29 Chris Nott and Richard Davies, "Digital Transformation in Defence – Balancing the Strategic and Tactical."

30 Department of National Defence, "VCDS Directive for CAF Digital Transformation – Draft."

31 Department of National Defence, "DefenceX – Defence Capabilities Blueprint," Government of Canada website, dated 1st December 2021, DEFENCEx - Defence Capabilities Blueprint (forces.gc.ca).

32 Ibid.

33 Lieutenant-Colonel Kenneth Bedley, "Closing the Tech Gap: A CAF Startup Model for Digital Transformation," Canadian Forces College, https://www.cfc.forces.gc.ca/papers/csc/csc47/mds/Bedley.pdf, p24.

Canada's key driver, the number of personnel deployed on operations will be reduced while still achieving the same, if not improved, operational objectives which are matched to meet the security threats presented.

This section has considered the CAF's approach to digital transformation. While the CAF is implementing its strategies based upon the Government of Canada's intent, it has highlighted that there remains disparity between the ambition, the resourcing, and the desire to learn upon industry to best grow the CAF digital transformation partnerships.

CAF Integration with Allies and NATO Partners

Having looked at the Government and the CAF perspectives for Canada, this section will now consider how their approaches to digital transformation are perceived from an international perspective, specifically focusing on partnerships with allies and NATO.

The CAF digital champion, Rear Admiral Zwick, stated that digital transformation at the very basic level is about credibility of defence to its allies, both on behalf of its population and international standing.[34] So, the CAF clearly understands the risks of not pursuing digital transformation, but what are its allies doing to address the same threats and challenges?

The Australian Defence Force's digital transformation strategy and agenda is mature and impressive. It is orientated entirely around meeting the strategic defence needs of Australia, determined by integral adjustment of communications and digital now being the warfighting environment of choice to empower faster decisions, rather than simply be enablers.[35] As such, their strategy is well funded, prioritised and understood across the force, offering a positive comparator and scale to where the CAF could aspire to deliver its digital transformation, if articulated against the security and operational risks, rather than just business processes.

In 2021 the UK Ministry of Defence invested another £10bn over 10 years into the central digital strategy aimed to create a digital backbone and community of digital specialists to respond to emerging security threats to defence.[36] However, even with high-level investment and clear strategic intent, the National Audit Office has expressed concerns that there is no overarching implementation plan nor ability to measure its

---

34 Terri Pavelic, "Operational Decisions at the Speed of Relevance," Vanguard Canada website, dated 22nd January 2023, Operational Decisions at the Speed of Relevance – Vanguard (vanguardcanada.com).

35 Australian Defence Force, "Ready to Fight and Win in the Digital Age: 2022 Defence Information and Communication Technology Strategy," Government of Australia, released in 2022, Defence-ICT-Strategy.pdf.

36 Committee of Public Accounts, "The Defence Digital Strategy," UK House of Parliament website, dated 3rd February 2023, The Defence digital strategy - Committee of Public Accounts (parliament.uk)

performance.[37] So while the UK aspirations are driven by the need to mitigate against security threats, this demonstrates the importance of viable implementation plans and the need of government departments to demonstrate what has been achieved before further investment is authorised;[38] a lesson identified by allies which could benefit the CAF, particularly in terms of early identification of performance indicators.

Without a surge in the digital transformation agenda of the CAF force right now, the CAF's allies will continue to evolve and potentially leave the CAF behind. Perhaps less well known, the traditional 5-Eye partnership have orientated themselves to now be talking in terms of data and embracing a culture of digital. Canada took the lead in developing the framework for the Force Operating Environment with 5-Eye partnership,[39] with key areas including enabling data innovation and analytics to prepare for the changing operating environment and security threats. From an alliance perspective, this had the opportunity to put Canada at the forefront of initiating the Government of Canada's intent through defence integration and to ensure Canada is integrated in novel defence technologies and is potentially an opportunity missed.[40] However, despite the 2018-19 report confirming the need to prioritise this activity, it wasn't until 2022 that the CAF released its first Digital Campaign Plan.[41] Although this could be attributed to the impact of Covid-19, but could also likely evidence the mismatch of ambition, prioritisation, and resource allocation the CAF has made towards digital transformation to date.

The 2022 AUKUS deal presents a prime example of how this delay in investment has left Canada outside of other key partnerships. Traditionally part of the 5-Eye partnership, Australia, the United States of America, and the UK have broken away to form their own alliance. While originally based upon a submarine deal, the partnership has expanded to including digital transformation and hosting technology to prepare for future evolutions in the digital realm.[42] From a defence commentary perspective, this was significant for Canada. Taking the submarine aspect away, the inevitable advancements of these three nation's partnerships will only serve to further distance Canada's ability to keep up with its allies and harm its reputation.[43] Seen by some critics as an accurate representation of how Canada has failed to strategize its defence policy and build

---

37 Lis Evenstad, "MOD Must Have a Clear Delivery Plan for Digital Strategy, says NAO," Computer Weekly website, dated 19th October 2022, MoD must have clear delivery plan for digital strategy, says NAO | Computer Weekly.

38 Chris Nott and Richard Davies, "Digital Transformation in Defence – Balancing the Strategic and Tactical."

39 Department of National Defense, "Future Force Design," Government of Canada website, dated 3rd July 2020, Future Force Design - Canada.ca.

40 Ibid.

41 Department of National Defense, "CAF Digital Campaign Plan."

42 Ministry of Defence and The Rt Hon Ben Wallace MP, "AUKUS Ministerial Joint Statement," UK Government website, dated 8th December 2022, AUKUS Defence Ministerial Joint Statement - GOV.UK (www.gov.uk).

43 Lee Berthiaume, "Armed Forces Concerned Over Canada's Absence from 'AUKUS' Security Pact," The Canadian Press, dated 15th January 2023, Armed Forces concerned over Canada's absence from 'AUKUS' security pact - National | Globalnews.ca.

appropriate momentum,[44] it also reemphasises the observation from the first part of this paper whereby Canada has so far failed to link the urgent requirement to prioritise digital transformation with its direct impact to national security. Without digital transformation being addressed in this way, the CAF faces a risk of a similar AUKUS situation and delaying digital transformation objectives in support of international interoperability.

Looking towards NATO, digital transformation has been identified as an essential enabler to achieve multi-domain operations. The NATO digital transformation strategy specifically noted the military could not achieve digital solutions in isolation and it must be a combination of academia, industry and coalition partnerships, which in turn have the ability to both shape culture and mitigate against security threats.[45] The CAF Digital Transformation Directive specifies the need to improve investment in digital transformation and integration with NATO but it will also be required to contribute knowledgeable digital skilled personnel and continuous support to NATO; without this commitment Canada will fail to retain its standing within NATO. Additionally, the CAF must invest in the digital infrastructure within Canada which will interconnect with NATO systems and enable access for all. With a reputation already publicly at risk with Canada's decision to invest less than the mandated 2% GDP to NATO, continued NATO interoperability focus is required for wider-CAF benefits.[46] Digital transformation in the context of NATO not only improves digital processing and analytics but provides innovate ways to improve interoperability with partners as well as industry and wider NATO partner nations; a reoccurring recommendation from academia working with military and industry.[47]

From a deployed scenario viewpoint, the CAF could now prioritise investment with its allies and NATO partnership, focusing on both preparing its homeland digital infrastructure whilst setting clear requirements to NATO development for digital objectives. As a result, the CAF could direct the digitalisation plan for the theatre deployment, being concurrently interoperable with partners and integrated with industry and wider Government of Canada departments relevant to the operation. The streamlined processes and organised data capture would allow faster decision making by all partners and the requirements for manual data transfers would be replaced by automation and AI technology. NATO, supported by the member nations, provides a secure and optimised digital enterprise for the battlespace.

This section has firstly considered the CAF's approach to digital transformation by comparison to approaches taken by its closest allies. It then highlighted the

---

44 Paul Mitchell, "Canada's Exclusion From the AUKUS Security Pact Reveals a Failing National Defence Policy," The Conversation website, dated 26th September 2021, Canada's exclusion from the AUKUS security pact reveals a failing national defence policy (theconversation.com).

45 NATO, "ACT Leads a Digital Transformation Workshop," NATO website, dated 13th January 2023, ACT Leads a Digital Transformation Workshop :: NATO's ACT.

46 Lee Berthiaume, "Budget: Canada Won't Meet NATO Target with New Military Funding."

47 Lyudmila Tolstolesova, Igor Glukhikh, Natalya Yumanova and Otabek Arzikulo, "Digital Transformation of Public-Private Partnership," Journal of Risk and Financial Management, Vol 14 number 121, p121, https://doi.org/10.3390/jrfm14030121.

opportunities of partnerships in the digital transformation realm but also noted partnerships where the CAF has failed to either influence or be included. These present risks to the CAF in terms of reputation, but more importantly, in their ability to rapidly address digital transformation in conjunction with their allies.

Benefits

This paper has identified the current approach to digital transformation by the CAF and the following key benefits that could be quickly realised if the CAF continues to invest and prioritise digital transformation activity:

Alignment of the CAF with pan-Government of Canada departments. Digital transformation offers a commonality between departments who all need to meet the Governments digital agenda targets. Partnerships will improve the speed of adaption, decision making responses and ability to better detect security threats to Canada and its allies.

Credibility. As a contributing nation who is both aware of security threats and has a resourced and supported digital transformation programme, the CAF is now recognised for its partnership contributions and becomes a partner of choice.

Interoperability. The CAF can direct and prioritise digital interoperability requirements, rather than needing to respond post decisions made by other allies and partners who were pre-positioned by their digital transformation prioritisation.

Commander's willingness. With a Digital Campaign Plan and Digital Transformation Directive, commanders are empowered to own their digital challenges, encourage innovation, and allow the CAF to enable digital transformation from the bottom up against well understood digital objectives.

Efficiencies in the number of CAF personnel. Digital transformation will streamline laborious processes across the CAF, reducing time taken and number of personnel who can now be reallocated against critical CAF capability support.

Recruitment and retention. The CAF is a digitally empowered force which accurately replicates the societal experience, rather than legacy defence digital capabilities, improving motivation and lived experience of CAF personnel.

Conclusion

This paper has demonstrated that without prioritisation of digital transformation by the CAF, it will fail to establish and endure partnerships with their allies, pan-government, and industry. To do this, the paper first outlined a potential deployment scenario for the CAF, orientating the reader to the situational challenges digital transformation needs to address for defence. The paper first addressed digital transformation from the Government of Canada's perspective, analysing their approach to global evolution of digital activity, how this has since been relayed into direction for pan-government departments, including the CAF and it also assessed the government's

alignment with industry as well as the impact of digital of Canada's population. The paper then reviewed the CAF's current response to digital transformation, including its Digital Campaign Plan and Digital Transformation Directive, in order to recognise the benefits it will deliver, while identifying gaps in their current approach such as industry engagement and prioritised funding. Finally, the paper considered the current perception of the CAF's approach to digital integration with its allies and partners by assessing their approaches to digital transformation and where there is alignment or divergence with strategies from the CAF. Throughout this paper, the deployment scenario was considered to highlight real-life benefits of digital transformation on behalf of defence outputs with the paper then summarising the direct benefits to the CAF organisation.

By analysing digital transformation from these three angles, the paper demonstrated that the CAF, enabled by the Government of Canada's intent, has all the momentum available to truly integrate and excel its approach to digital transformation. It must however continuously evolve its approach to learn from the lessons identified by its allies, NATO, and industry in order to truly remain at the forefront of its evolution, and more importantly, prioritise the resources required to enable this.

In parallel, the Government of Canada must now begin to frame the potentials of digital in terms of security threat mitigation to ensure the motivations behind the digital transformation are guided by the ambition to strive to be a leading defence partner rather than realising too late that digital and security threats are not integrated. Failure to do so will result in the CAF, as demonstrated in their exclusion from partnerships such as AUKUS, being self-relegated to the status of less than favourable coalition partners. This alone should be a wake-up call for the Government of Canada and the CAF to act now to avoid losing its promised momentum to achieving digital transformation. If this CAF does not like change, it will like irrelevance even less.

BIBLIOGRAPHY

Agius, C. "Social Constructivism." Contemporary Security Studies. Sixth edition. Oxford University Press (2022).

Aidrous,I, Asmyatullin,R and Glavina,S, "The Development of the Digital Economy: GCC Countries Experience." Industry Competitiveness: Digitalization, Management, and Integration. ISCI 2019. Lecture notes in Networks and Systems. Vol 280. Dated 15th August 2021. https://doi-org.cfc.idm.oclc.org/10.1007/978-3-030-80485-5_21 .

Australian Defence Force. "Ready to Fight and Win in the Digital Age: 2022 Defence Information and Communication Technology Strategy." Government of Australia. Released in 2022. Defence-ICT-Strategy.pdf.

Berthiaume,L. "Armed Forces Concerned Over Canada's Absence from 'AUKUS' Security Pact." The Canadian Press. Dated 15th January 2023. Armed Forces concerned over Canada's absence from 'AUKUS' security pact - National | Globalnews.ca.

Berthiaume,L. "Budget: Canada Won't Meet NATO Target with New Military Funding." CTV News. Dated 7th April 2022. Budget: Canada won't meet NATO target with new military funding | CTV News.

Buchanan, J, Kelley, B and Hatch, A. "Digital Workplace and Culture: How Digital Technologies are Changing the Workforce and How Enterprise Can Adapt and Evolve." Deloitte website. Dated 2016. us-cons-digital-workplace-and-culture.pdf (deloitte.com).

Committee of Public Accounts. "The Defence Digital Strategy." UK House of Parliament website. Dated 3rd February 2023.The Defence digital strategy - Committee of Public Accounts (parliament.uk).

Department of National Defense. "Canadian Armed Forces Digital Campaign Plan." Government of Canada website. Dated January 2023. CAF_Digital_Campaign_Plan.pdf (canada.ca).

Department of National Defense. "DefenceX – Defence Capabilities Blueprint." Government of Canada website. Dated 1st December 2021. DEFENCEx - Defence Capabilities Blueprint (forces.gc.ca).

Department of National Defense. "CAF Digital Campaign Plan." Government of Canada website. Dated 22nd February 2023. CAF_Digital_Campaign_Plan.pdf (canada.ca).

Department of National Defense. “Future Force Design.” Government of Canada website. Dated 3rd July 2020. Future Force Design - Canada.ca.

Department of National Defense. “Strong, Secure and Engaged.” Government of Canada website. Released in 2017. Strong, Secure, Engaged. Canada's Defence Policy.

Department of National Defense. “VCDS Directive for CAF Digital Transformation – Draft.” Government of Canada. Document number 10711984. Version 27. Dated 22 December 2022.

Engen,R. “When the Teeth Eat the Tai: A Review of Canada’s Defence Artificial Intelligence.” Defence AI Observatory. Dated January 2023. DAIO_Study2309.pdf (defenseai.eu).

Evenstad,L. “MOD Must Have a Clear Delivery Plan for Digital Strategy, says NAO.” Computer Weekly website. Dated 19th October 2022. MoD must have clear delivery plan for digital strategy, says NAO | Computer Weekly.

Gillor, H. “Digital transformation: An Unstoppable Global Megatrend.” Institute for Digital Transformation. Dated 5th February 2018. Digital transformation – An Unstoppable Mega Trend (institutefordigitaltransformation.org).

Girard,M. “Global Standards for Digital Corporation.” Centre for International Governance Innovation. Dated 28th October 2019. Global Standards for Digital Cooperation - Centre for International Governance Innovation (cigionline.org).

Kravchenko, O. ‘Digitalization as a Global Trend and Growth Factor of the Modern Economy.” Bohdan Khmelnytsky National University of Cherkasy. Ceur Vol 2422. Dated May 2019. paper35.pdf (ceur-ws.org).

Kent,S. “Digital Transformation: Digital Banking Strategies.” Blog on CSI Web. Dated 24th November 2021, Digital Transformation: Digital Banking Strategies Throughout the Customer Lifecycle | CSI (csiweb.com).

Lieutenant-Colonel Kenneth Bedley. “Closing the Tech Gap: A CAF Startup Model for Digital Transformation.” Canadian Forces College. https://www.cfc.forces.gc.ca/papers/csc/csc47/mds/Bedley.pdf.

Ministry of Defence and The Rt Hon Wallace,B MP. “AUKUS Ministerial Joint Statement.” UK Government website. Dated 8th December 2022. AUKUS Defence Ministerial Joint Statement - GOV.UK (www.gov.uk).

Mitchell,P. “Canada’s Exclusion From the AUKUS Security Pact Reveals a Failing National Defence Policy.” The Conversation website. Dated 26th September 2021. Canada's exclusion from the AUKUS security pact reveals a failing national defence policy (theconversation.com).

NATO. “ACT Leads a Digital Transformation Workshop.” NATO website. Dated 13th January 2023. ACT Leads a Digital Transformation Workshop :: NATO's ACT.

Nott,C and Davies,R. “Digital Transformation in Defence – Balancing the Strategic and Tactical.” IBM UK and Ireland website. Dated 18th November 2021. Digital Transformation in Defence - Balancing the Strategic and the Tactical - IBM UK & Ireland - Blog

Pavelic,T. “Operational Decisions at the Speed of Relevance.” Vanguard Canada website. Dated 22nd January 2023. Operational Decisions at the Speed of Relevance – Vanguard (vanguardcanada.com).

Raytheon Missiles and Defence. “Digital Transformation.” Raytheon website. Last accessed 3rd May 2023. Digital Transformation | Raytheon Missiles & Defense (raytheonmissilesanddefense.com).

Scarborough,M. “4 Megatrends Shaping Post-Pandemic Digital Transformation.” Business Development Bank of Canada. Dated 2021. 4 megatrends shaping post-pandemic digital transformation | BDC.ca.

Tolstolesova,L, Glukhikh,I, Yumanova,N and Arzikulo,O. “Digital Transformation of Public-Private Partnership.” Journal of Risk and Financial Management. Vol 14 number 121.https://doi.org/10.3390/jrfm14030121.

Treasury Board of Canada Secretariat. “Digital Ambition 2022.” Government of Canada website. Dated 2022. Canada’s Digital Ambition 2022 - Canada.ca.

Treasury Board of Canada Secretariat. “Digital Operations Strategy 2021 – 2024.” Government of Canada website. Dated 2021. Digital Operations Strategic Plan: 2021–2024 - Canada.ca.

UK Department of Digital, Culture, Media and Sport. “UK Digital Strategy.” UK Government website. Dated 04 October 2022. UK Digital Strategy - GOV.UK (www.gov.uk).

Vallance,C. “TUC: Government Failing to Protect Workers from AI.” BBC News website. Dated 17th April 2023. TUC: Government failing to protect workers from AI - BBC News.