National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Cloud-Enabled Decision Advantage Within the Canadian Armed Forces

Lieutenant-Colonel Suraj R. Akolkar

JCSP 49 DL

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 49 AD

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 DL - PCEMI n° 49 AD
2022 - 2024

Exercise Solo Flight – Exercice Solo Flight

Cloud-Enabled Decision Advantage Within the Canadian Armed Forces

Lieutenant-Colonel Suraj R. Akolkar

Cloud-Enabled Decision Advantage Cloud Within the Canadian Armed Forces

INTRODUCTION

In the book *Four Battlegrounds*, the author Paul Scharre quotes Chinese President Xi Jinping that: "Science and technology has become the main battleground of global power rivalry."[1] The book argues that since "power is the currency of international relations,"[2] there are four main elements of data, technology (specifically computing power), talent, and institutions that are essential for power. This assessment by Scharre seems valid and it is acknowledged that the Canadian Armed Forces (CAF) is also modernizing its Defence Strategy by changing its institutional and operational approaches. At the institutional level, the CAF has released documents such as the CAF Digital Campaign Plan, the CAF Artificial Intelligence Strategy, and the Joint Intelligence, Surveillance, and Reconnaissance – Future Operating Concept. The CAF is also modernizing its operational approach with its Pan-Domain Force Employment Concept (PFEC). The documents provide threat analysis to CAF leaders of our adversaries' capabilities (especially China and Russia) who use all instruments of national power – Diplomatic, Information, Military, and Economic (DIME) to weaken our ability to defend ourselves. As the PFEC notes, "If Canada and its allies fail to respond to this mounting competition, uphold our democratic principles, and preserve the RBIO [Rules-Based International Order], these adversaries will increasingly gain military, technological, and economic advantages."[3] Therefore the aim of this paper is to provide a solution that can help the CAF to counter these challenges in the future.

The recently released Pan-Domain Command and Control (PDC2) concept within the PFEC, explains that: "We must evolve to a Pan-Domain C2 approach that integrates intelligence and information from a variety of sensors and sources from across domains, makes sense of this data, and distributes it to enable decision-makers."[4] The main capability gap that PFEC highlights is the reduced ability (or inability in some cases) of CAF commanders to achieve decision advantage in a battlespace due to lack of Situational Awareness (SA) and Shared Understanding (SU). The PDC2 concept is about connecting sensors and data sources to effectors as indicated in Figure 1 below.[4]

---

[1] Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: WW Norton, 2023)..

[2] *Ibid*., 23.

[3] Canada. Department of National Defence, *Pan-Domain Force Employment Concept: Prevailing in a Dangerous World* (Ottawa, ON: Department of National Defence, 2023), 13.

[4] *Ibid*, 28..

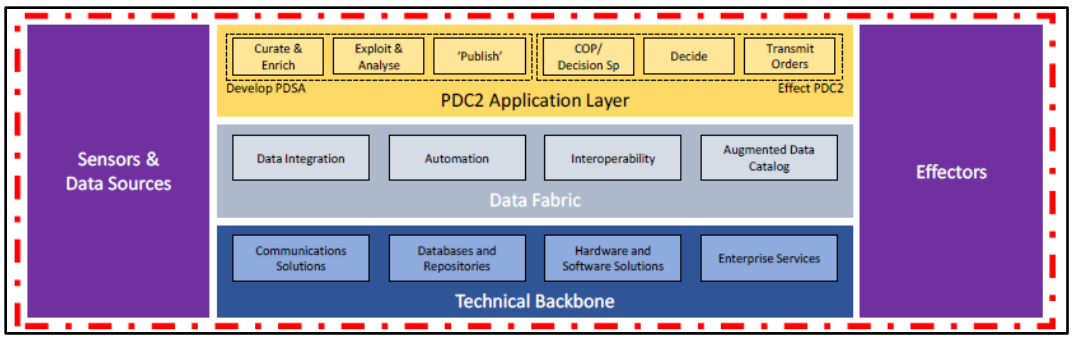

Figure 1: Pan-Domain C2 concept.

Source: Pan-Domain Force Employment Concept.

Effective and efficient PDC2 requires robust and resilient communication systems that are commonly referred to as Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. As mentioned in the PFEC, the characteristics of the operating environment have changed. First, state and non-state actors are increasingly operating in a grey space of conflict where there is an overlap of interests due to a power competition between states. The CAF will have to excel in this grey space to project military power, and C4ISR systems are vital enablers. Secondly, the changing characteristics of conflict mean that the CAF will not be the only player in the grey space and will have to rely on Other Governmental Departments (OGD) and allies. This will require C4ISR systems that are not only *interoperable* between OGDs and allies but also capable of moving information rapidly and securely to relevant decision makers. Thirdly, the rapid evolution of technology has significantly improved computing power to enable functions such as analytics, artificial intelligence, virtual reality, robotics, and big data storage and processing. This has enabled rapid processing of data to be provided to decision makers using the C4ISR systems. And finally, alignment of C4ISR systems with our allies is required to participate in combined and joint operations. All of this has meant that future military operations will depend on how effectively and efficiently data is used by military commanders to accelerate their decision process and maintain Command and Control (C2) in a dynamic battlespace.

THESIS STATEMENT

This essay will argue that *cloud adoption within the CAF is essential for providing decision advantage* to CAF commanders during operations based on the threat picture portrayed in the Pan-Domain Force Employment Concept.

DISCUSSIONS

Figure 2 below, depicts how sensors are connected to effectors through C4ISR systems from the tactical level to the operational level in the context of Canadian Special Operations Forces (CANSOF), but can be representative of other CAF elements. The key component that enables sensors to ‘talk to’ effectors are tactical and enterprise networks which form the technical backbone[4] of the C4SIR capability.

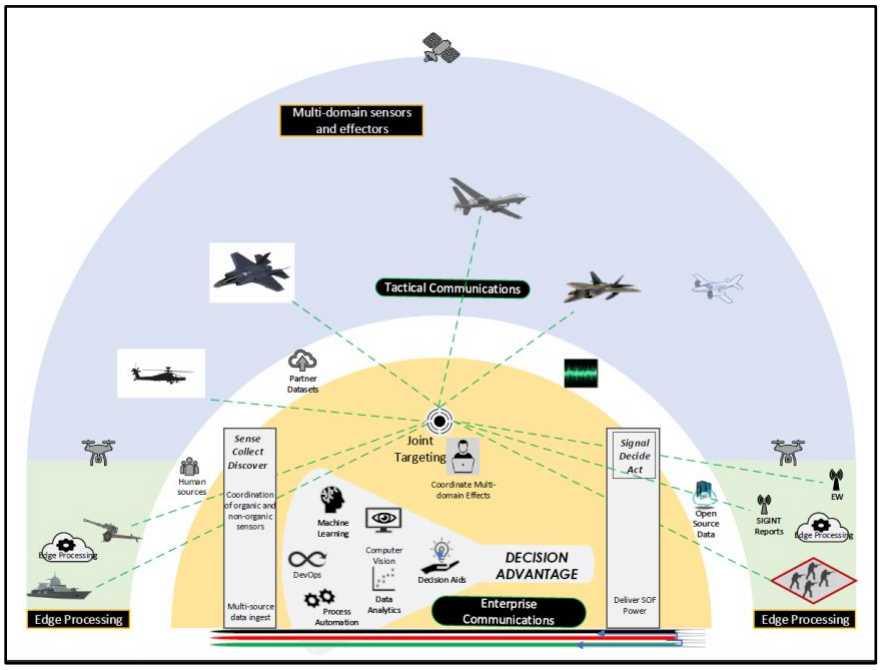

Figure 2: A typical SOF C4ISR Network.

Source: SOF C4ISR Graphic created by project team.

As indicated in Figure 2 above, data must flow rapidly and securely across various systems through communication pathways, be automatically processed (either at the edge or operation centres) to provide the appropriate information and intelligence to commanders at different levels to enable their decision-making. To achieve this, a *cloud* will better enable and aid commanders to make decisions much faster due to the availability of right data at the right time compared to current methods.

What is a Cloud?

In simple terms, a cloud brings many Information and Communications Technologies (ICT)[5] together as depicted in Figure 3 below.

[5] Kritika Roy, *Advances in ICT and the Likely Nature of Warfare* (New York, N.Y.: Routledge, 2020).

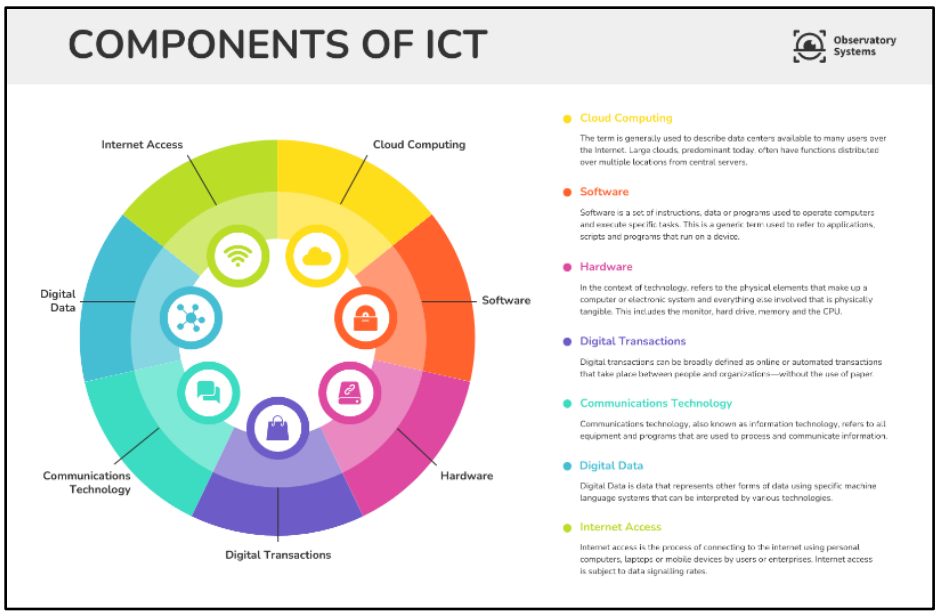

Figure 3: Components of ICT.

Source: Advances in ICT and the Likely Nature of Warfare.

A cloud includes traditional virtualization solutions and is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [6] There are five essential characteristics of cloud that enable effective and efficient exchange of data across various domains rapidly to enable decision advantage for commanders. First, is *on-demand self-service*, which is defined by NIST as automatic and near-instantaneous unilateral access to computing capabilities such as hardware, software, servers, storage capacity etc. as required, without human intervention. Second, is *broad network access*, which consists of availability of various communication pathways that can link various sensors and devices to information exchange gateways. Third, is *resource pooling*, which includes pooling of various computing resources (such as storage solutions, processing, memory, network bandwidth etc.) "to serve multiple consumers using a multi-tenant model with different physical and virtual resources that are dynamically assigned and reassigned according to consumer demand."[7] Fourth, is *rapid elasticity*, which is defined as the ability to expand the required resources in a way that is transparent to the consumer. The consumer does not have to worry about running out of storage space or computing power during their usage. And finally, *measured service*, which is defined as the ability to automatically control, monitor, and optimize resources such that a customer is

[6] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing" (Gaithersburg, MD: U.S. Department of Commerce, September 28, 2011), 2, https://doi.org/10.6028/NIST.SP.800-145.

[7] *Ibid.*

charged in a pay-per-use model to reduce costs. Measured service could also facilitate use of AI/ML technologies to provide autonomous processing of data.

Types of Cloud

When talking about cloud, there are two aspects that need to be considered: the service model (details the 'what') and the deployment model (details the 'how') of a cloud. There are three types of service models: *Software as a Service (SaaS)*, *Platform as a Service (PaaS)*, and *Infrastructure as a Service (IaaS)*.[6] The service models provide various levels of the five essential characteristics of the cloud mentioned above within a cloud product. On the other hand, the deployment models of a cloud focus on who owns the cloud product and establishes relevant controls on storage of data. There are four types of deployment models: *private cloud* (used by a single organization), *community cloud* (used by a specific community of users), *public cloud* (use by public), and *hybrid cloud* (combination of private, community, or public deployment models). In addition, a cloud could be deployed *on the premises of an organization* (on-prem) or *on the premises of the cloud provider* (off-prem).[6] Figure 4 below explains the concept of shared responsibility in the cloud.

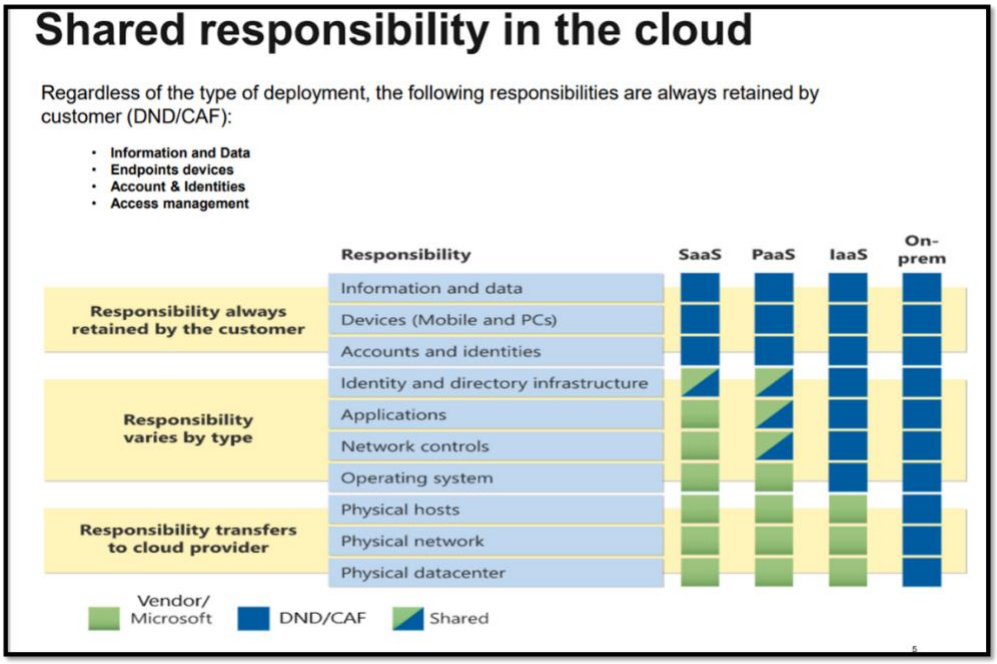

Figure 4: Ways to deliver services in a cloud.

Source: Associate ADM (CIO) PowerPoint presentation on cloud.

What is Decision Advantage?

This paper will use Special Operations Forces C4ISR project (SOF C4ISR) as a use case example to explain the concept of decision advantage during military operations using two scenarios: tactical level and operational level. The draft business case analysis (V1) defines decision advantage "as the expertise and resources to source, access, process, evaluate, display,

and distribute information" [8] to commanders at various levels. Building this Common Operating Picture (COP) is one aspect of decision advantage. Figure 5 below explains the C4ISR decision advantage model in the context of the SOF C4ISR project.

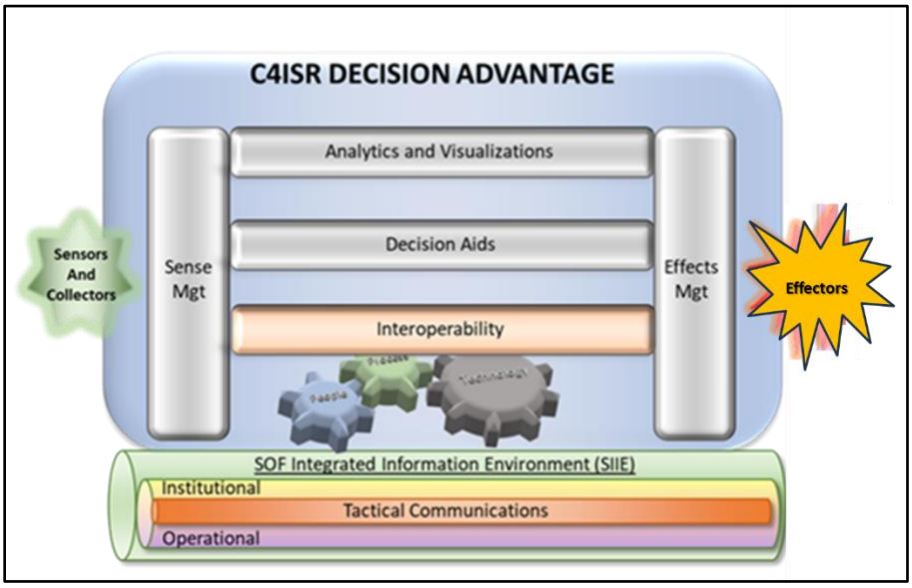

Figure 5: C4ISR Decision Advantage model.

Source: SOF C4ISR – Business Case Analysis V1.0.

Another aspect of decision advantage is getting data from sensors and collectors to effectors as rapidly as possible. It is about conducting our Observe, Orient, Decide, and Act (OODA) loop faster than our adversaries. These two aspects combined provides decision advantage to commanders. As depicted in Figure 2, data collected from sensors is brought to a ground station and moved into a telecommunications network. In the context of CANSOF, this network is called the SOF Integrated Information Environment (SIIE). In simple terms, SIIE consists of the various unclassified to classified networks that connect the tactical, operational, and strategic levels and forms the technical backbone. The data from the various sensors is collected, tagged, wrapped, processed, and put into storage devices to be analysed. This process is called Sense management and is the method of building SA and SU as required. As depicted in Figure 4, depending on the type of cloud service, a lot of the Sense management process can be automated to provide relevant information at a much faster rate than current methods. Analytics and visualization tools, decision aids, and interoperable networks are tools that bring SA and SU to decision makers. For example, in the FVEYs and NATO environments, this passage of information would be accomplished through the Federated Mission Networks (FMN). FMN is a global environment built on common IM/IT standards, policies, governance, technology, and tactics, techniques, and procedures (TTPs). By implementing FMN, C4ISR networks will be 'day one ready' when deployed to operations. Cloud technology's characteristics of on-demand

[8] SOF C4ISR Project Team, *SOF C4ISR - Business Case Analysis V1.0*, (Draft) (Ottawa: Department of National Defence, 2024).

self-service, broad network access, and resource pooling makes it easier to meet FMN standards compared to current methods. The COP that is developed in Sense management is then presented to decision-makers in Effects management. Effects management essentially deals with the targeting process of developing target packages, getting them approved, and delivering them to effectors for execution. The decision-making process happens here and therefore this node is the centre of gravity in providing decision advantage to commanders. For example, Full-Motion Video (FMV) is one capability that is requested by commanders during operations. In the current state, FMV feeds from various sensors (mostly manned and unmanned aircrafts and Unmanned Aerial Vehicles (UAV)) are brought into the respective networks of nations and then into a common operational network by Cross-Domain Solutions (CDS). It takes time to build CDS and if they are not properly configured, the flow of data can be interrupted. This lack of interoperability would mean that decision-makers in Effects management would have only partial information to make decisions. With implementation of Data Centric Security (DCS) and Zero Trust Framework (ZTA)[9], the need for CDS is reduced as only the personnel with the appropriate Identity Credentials and Access Management (ICAM) would be able to access the data. In the case of the FMV example, it would mean that at the beginning of the mission, all nations in the coalition would have access to the live feeds from a UAV. As the UAV moves into certain geographical areas, only certain personnel would be able to access the feeds depending on their ICAM (e.g. FVEY). In this way while the data is available within the network, accessing the data is not possible without the appropriate ICAM.

SOF Scenarios to explain Decision Advantage

Two operational scenarios have been developed to explain the use of cloud in providing decision advantage to commanders at the operational level and the tactical level.

[9] Boury-Brisset, A.-C. (2021). *Internet of Things (IoT) architectures with fog/edge computing.* Ottawa: Defence Research and Development Canada.

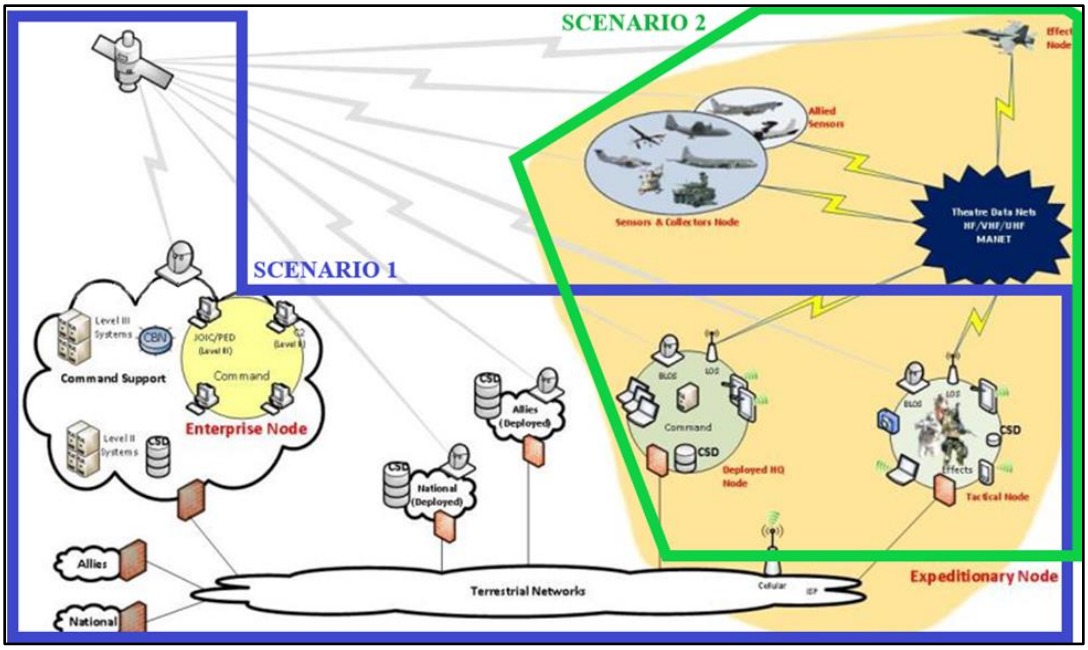

Figure 6: Operational View Level 1 diagram (OV-1) within the NCM.

Source: SOF C4ISR – Business Case Analysis V1.0.

At the Operational level, the SIIE extends from the enterprise node of the respective national networks of nations to their expeditionary nodes of their deployed systems through terrestrial networks. In essence, it is the extension of the various national systems of a country to their deployed operational headquarters. Figure 6 scenario 1 (blue boundary) depicts the current network model of this concept.[8] The SIIE would be built/configured to the relevant FMN standards of the operation to enable interoperability. There are two main issues/challenges with the above model in providing decision advantage to commanders. First, there is a big assumption that all the allied nations would build/configure their networks to the agreed upon FMN standards. Incorrect FMN standards would result in interoperability issues and reduces (or stops) information flow between various operational networks, such that commanders will not have all the information that they need to make effective decisions. As explained above, cloud technology can reduce interoperability issues by enabling flow of data but limiting access based on ICAM of users. Second is limitation in availability of processing and storage capabilities at the deployed operational level. Faster OODA loop means faster ability to process data, and this requires computing capabilities. Cloud's characteristic of rapid elasticity and measured service could provide ways to push AI/ML technologies to the operational level and assist in processing data with limited human intervention. Similarly, resource pooling and on-demand self-service would provide unlimited storage space, computing power, applications for building COP and targeting purposes.

At the Tactical level, the SIIE is focused on execution of warfare (fires) and therefore only require systems that are needed to complete the tactical missions. The primary methods of communication are MANet (Mobile Ad-hoc Networks) that form a mesh network using various bearers such as 4G/5G, radios, Satcom etc. These networks are generally required for short,

discrete periods in extremely localized regions and are heavily constrained by bandwidth. As depicted in Figure 6 scenario 2 (green boundary), tactical nodes are setup to bring information forward to the warfighter. The two main issues/challenges at the tactical level are automated passage of relevant information and bandwidth. Edge cloud devices can enable availability of the right information at the right time by using AI/ML algorithms to process data and reducing (or removing the need to be connected to backend systems for accessing data. For example, Breqwatr cloud stack[10], can be used as a storage device, application server, chat server, etc. into one device as opposed to having separate devices for each function. This allows tactical edge processing of data without reliance on backend systems. This is advantageous in low bandwidth environments at the tactical level.

In this manner, the inherent characteristics of cloud can remove the barriers mentioned above and enable rapid decision- making by commanders. Figure 7 below maps some of the layers of the current network model of the C4ISR systems to the cloud. It is not possible to depict beyond the network layer of the cloud with the OV-1 scenario diagram due to the visual aid limitations. The intent is to show that decision advantage is achieved by the cloud due to the five essential characteristics of the cloud mentioned above. Since all the data from the sensors is centralized within the cloud (layer 4 – computing and storage platforms), AI/ML applications (layer 5 – cloud and enabling services) can be deployed to rapidly and sort through data from various domains (layer 6 – multi-domain data fabric) and provide the relevant COP in near-real time (layer 7 – information advantage). This provides decision advantage (layer 8) to commanders during operations.

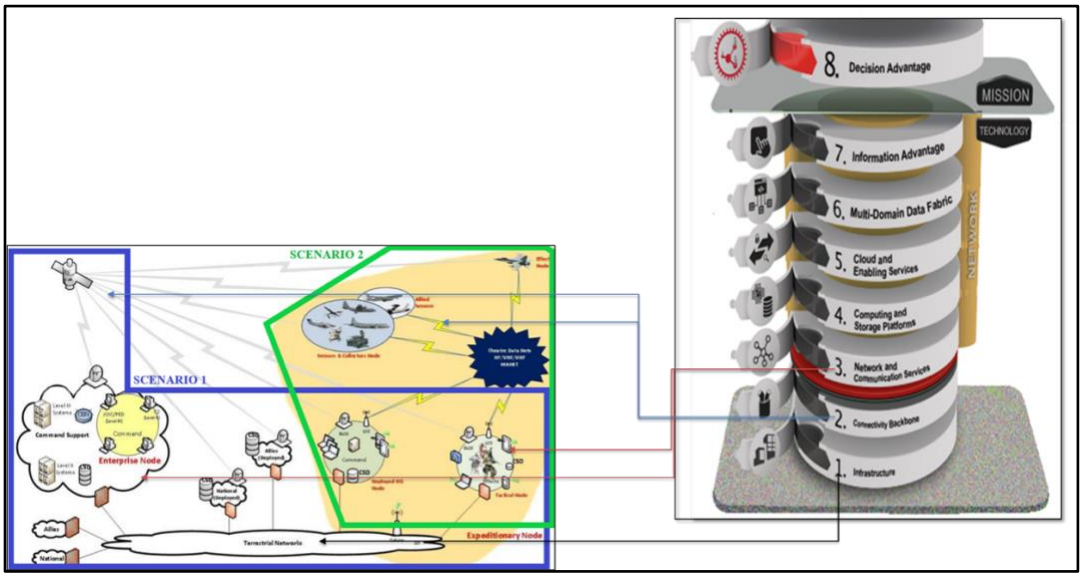

Figure 7: Mapping of some functions of NCM to cloud.

Source: SOF C4ISR – Business Case Analysis V1.0.

[10] SOF C4ISR Project Team. 2024. *What is Breqwatr Cloud and why do I care.* PowerPoint Presentation, Ottawa: Department of National Defence.

CONCLUSION

The CAF is at an operational disadvantage due to the inability of its commanders to gain decision advantage in a battlespace. This situation is concerning as our adversaries, especially China and Russia are using DIME to weaken our ability to defend ourselves and be a valuable contributing partner to our allies. Cloud technology has the potential to provide decision advantage to CAF commanders due to its inherent characteristics and deployment model.

Cloud operates on a shared responsibility concept such that military commanders can pick and choose the services they require in the battlespace depending on the circumstances. Cloud can enable processing at the edge and in tactical environments without having to continuously rely on national backend systems for processing of information or data. Depending on the type of cloud, it is possible for cloud providers to deploy AI/ML algorithms to aid commanders from making quick decisions. As discussed in this paper, cloud technology offers various options to users, and it is important that CAF develops its cloud capabilities with an informed threat picture as presented in the PFEC. It is recommended that in the near term, various elements within the CAF should participate in Project OLYMPUS activities which have been directed by the Vice Chief of the Defence Staff (VCDS) to develop cloud technologies.

References

Boury-Brisset, Anne-Claire. 2021. *Internet of Things (IoT) architectures with fog/edge computing.* Ottawa: Defence Research and Development Canada.

Department of National Defence. 2022. *Canadian Armed Forces - DIGITAL CAMPAIGN PLAN.* Ottawa: DND.

Department of National Defence. 2022. *Joint Intelligence, Surveillance, and Reconnaissance - Future Operating Concept.* Ottawa: DND.

Department of National Defence. 2024. *Pan-Domain Force Employment Concept.* Ottawa: DND.

Department of National Defence. 2022. *The Department of National Defence and Canadian Armed Forces - Artificial Intelligence Strategy.* Ottawa: DND.

Mell, Peter, and Timothy Grance. 2011. *The NIST Definition of Cloud Computing.* Gaithersburg: U.S. Department of Commerce.

Payne, Kenneth. 2021. *I, Warbot - The Dawn of Artificially Intelligent Conflict.* New York: Oxford University Press.

Roy, Kritika. 2020. *Advances in ICT and the Likely Nature of Warfare.* New York: Routledge.

Scharre, Paul. 2023. *Four Battlegrounds - Power in the Age of Artificial Intelligence.* New York: W.W. Norton & Company Ltd.

SOF C4ISR Project Team. 2024. *SOF C4ISR - Business Case Analysis V1.0 (Draft).* Ottawa: Department of National Defence.

SOF C4ISR Project Team. 2024. *What is Breqwatr Cloud and why do I care.* PowerPoint Presentation, Ottawa: Department of National Defence.