National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CLOUDS ON THE HORIZON: A CASE FOR CLOUD COMPUTING IN THE ROYAL CANADIAN NAVY

Lieutenant-Commander Greg R. Zuliani

JCSP 45

Service Paper

Disclaimer

PCEMI 45

Étude militaire

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 45 – PCEMI 45
15 October 2018

DS 545 Component Capabilities

CLOUDS ON THE HORIZON: A CASE FOR CLOUD COMPUTING IN THE ROYAL CANADIAN NAVY

By LCdr Greg R. Zuliani

CLOUDS ON THE HORIZON: A CASE FOR CLOUD COMPUTING IN THE ROYAL CANADIAN NAVY

AIM

1. Cloud computing has become increasingly common throughout industry, government departments, and society in general. There is a somewhat broad-spectrum understanding of just what exactly cloud computing is and recently discussions have turned to how the Canadian Armed Forces (CAF) can best make use of these types of technology.[1] This includes leveraging the massive amounts of data collected, sometimes referred to as "big data", by using analytics to more effectively inform commanders. This service paper aims to demonstrate how cloud computing could provide practical information technology (IT) infrastructure to manage the significant amounts of data collected by ships, maritime helicopters, boats, and unmanned aircraft of the current and future fleets of the Royal Canadian Navy (RCN).

INTRODUCTION

2. The RCN's operating environment presents a set of unique challenges that are largely not faced by the other elements. Once a ship proceeds to sea, all connectivity through the Defence Wide Area Network (DWAN) and any other network onboard is reliant upon satellite communications. The Government of Canada (GC) defines cloud computing as "…the delivery of computing services — servers, storage, databases, networking, software, analytics, and more — over the Internet".[2] This traditional understanding and implementation of cloud computing that takes for granted a constant and reliable connection may not be the ideal fit for the RCN.

[1] Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy*. (Ottawa: National Defence, 2017), 55.

[2] Shared Services Canada. "Cloud Computing." Last accessed 13 October 2018. https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html

However, industry is developing innovative ways to leverage private, on premises, cloud-based solutions that have the potential to vastly change the way the RCN handles data.

3. Advanced sensor systems such as the RCN Intelligence, Surveillance, Target Acquisition and Reconnaissance Unmanned Aircraft System (RCN ISTAR UAS)[3] and the Multi Role Boat (MRB)[4] will feed massive amounts of data back to the ship that will require processing, exploitation, and dissemination. In addition to the data already collected by a ship at sea, these systems and others will increase the data management requirements beyond current capacity. In light of the connectivity limitations noted above, the RCN requires an innovative way to manage information onboard a single ship as well as amongst a task group and ultimately the fleet as a whole.

DISCUSSION

4. In making the case for cloud computing, this paper will begin by exploring big data's size, scope, and opportunities for the RCN. Potential existing solutions and how they could fit in with the RCN's existing and future fleet will then be briefly examined. Finally security concerns and current government policy will be addressed before arriving at recommended courses of action for the RCN moving forward.

Size, Scope, and Opportunities

5. Big data is a term that is widely used and has a tendency to be seen by some as just a vague and trendy buzzword. Of the various definitions available, IBM offers one that captures the essence of the problem as follows "Big data is a term applied to data sets whose size or type is beyond the ability of traditional relational databases to capture, manage, and process the data

---

[3] Department of National Defence. "Defence Capabilities Blueprint: Royal Canadian Navy Intelligence Surveillance Target Acquisition and Reconnaissance Unmanned Aircraft System." Last accessed 13October 2018. http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1297

[4] Department of National Defence. "Defence Capabilities Blueprint: Multi Role Boat." Last accessed 13October 2018. http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=941

with low-latency."[5] This definition is helpful as it captures the fact that various types of data (such as full motion video, signals intelligence, and a vessel's track history) must be handled simultaneously and it also highlights the importance of processing that data with low-latency. Processing the collected data days or weeks after it was collected is useful for determining patterns over a period of time, but does little to help the in-situ commander at the time of collection.

6. To better illustrate the sheer size of the problem, the P8-A *Poseidon* maritime patrol aircraft collects between five and eight terabytes of data *per sortie*.[6] Moving this amount of raw data ashore to be processed in a timely manner is just not feasible given that transferring a single terabyte of data using a 50 Megabit per second (Mbps) satellite link would take approximately three days.[7] Therefore, any solution to the big data problem facing the RCN must be able to ingest massive amounts of data and conduct some level of initial processing of that data such that it is searchable and useable to analysts both onboard and ashore. This initial processing could be something as simple as ensuring the proper meta-data is attached to the files so that they can be effectively searched and managed. This type of solution sounds relatively straightforward when considering a single ship operating independently; download the data to an onboard server and send only the required data to analysts ashore. However, the problem becomes quite a bit more complex when considering multiple ships operating together in a naval task group.[8]

7. Sharing a recognized maritime picture is a fundamental aspect of operating as part of a task group and one of the keys to the group's effectiveness. Being able to employ sensors across

[5] IBM. "Big Data Analytics." Last accessed 13 October 2018. https://www.ibm.com/analytics/hadoop/big-data-analytics

[6] United States. Department of the Navy. *Maritime ISR Enterprise Acquisition (MIEA) Review.* (Washington, DC: U.S. Government Printing Office, 2011), 20.

[7] *Ibid, 11.*

[8] "Composed of up to four surface combatants and a joint support ship, and supplemented where warranted by a submarine…" Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy*. (Ottawa: National Defence, 2017), 35.

the entire group extends the situational awareness of the task group commander out beyond his/her own ship. This should also be the case with advanced sensors like unmanned aircraft or maritime helicopters. Not every ship in the task group will carry an unmanned aircraft or maritime helicopter, but they should be able to benefit from the cumulative sensor data from these platforms. For example, to get imagery from a CH-148 *Cyclone* to the remainder of the task group, the host ship would have to upload the imagery to a central location where the other ships could then access it or email it directly to individuals. Neither of these solutions is ideal and as discussed above, it is impractical to transfer much more than still images via satellite links. This problem is only compounded when multiple ships need to upload and download the same data.

8. The RCN recognizes the reality that innovation will be required to solve this problem; the Strategic Plan specifically notes that "Managing big data, limited bandwidth, and the cyber vulnerability that this entails, will demand thinking and approaches that break with traditional mindsets."[9] One innovative way of approaching this problem would be through the concept of a tactical cloud specifically for the task group. In a nutshell, this would result in a localized private cloud amongst the task group that would provide adequate storage and processing at sea and would be able to eventually synchronize with another master cloud ashore.[10] This approach allows the sharing of data between ships operating together as a task group while eliminating the requirement for ships to individually reach back and synchronize to one master cloud ashore. An additional benefit would be the potential to use other means to transfer data across the smaller

---

[9] Canada. Department of National Defence. *Royal Canadian Navy Strategic Plan 2017-2022.* (Ottawa: National Defence, 2017), 9.

[10] Wilson, Bradley, Isaac R. Porche III, Mel Eisman, Michael Nixon, Shane Tierney, John M. Yurchak, Kim Kendall, James Dryden and Sean Critelli. *Maritime Tactical Command and Control Analysis of Alternatives. (*Santa Monica: RAND Corporation, 2016), 14.

distances of a task group such as fifth generation (5G) cellular or ad-hoc mesh networks. These types of networks could allow ships to join and leave the network dynamically at sea similar to the way in which cell phones join and leave available Wi-Fi networks.

9. The same concept could also be elevated to the fleet level. Ships that deploy with their own tactical cloud would return to port and synchronize their data with a master fleet level or even CAF level cloud. Once alongside, ships would be able to connect to land-based networks and transfer massive amounts of collected data in a practical manner. Once synchronized with the shore based cloud, the aggregate data of multiple deployments could then be run through software analytics to identify trends or patterns that would otherwise go unnoticed. For example, perhaps over a series of ten Op *Caribbe* deployments the data collected could show that in the summer months traffickers generally use a specific route whereas in the winter months an alternate route is used. This type of long-term analysis of patterns of life in the area of operations is only one example of the benefits that would be realized through the use of cloud computing and analytics. With advances in machine learning and advanced algorithms, there are surely other patterns that could be discerned and exploited for future operations.

Existing Solutions

10. The concept described above may seem aspirational and implausible to implement in the RCN. However, a number of industry partners have already developed or are in the process of developing solutions that could be implemented in a relatively straightforward manner. Cloud-based solutions for customers with intermittent connectivity have been developed by both world leaders in cloud computing; Microsoft and Amazon Web Services.[11] Both Azure Stack by Microsoft and Snowball Edge by Amazon offer on-premises data storage, synchronization with

[11] Forbes. "The Top 5 Cloud-Computing Vendors: #1 Microsoft, #2 Amazon, #3 IBM, #4 Salesforce, #5 SAP. Last modified 7 November 2017. https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing vendors-1-microsoft-2-amazon-3-ibm-4-salesforce-5-sap/#3a2d3b426f2e

their respective parent cloud services, and both local and cloud-based analysis and processing. This hybrid-model of cloud computing allows for the best of both worlds in leveraging the power of cloud computing when feasible while simultaneously allowing for limited connectivity and pushing significant storage and processing power to the edge. Implementation of a system similar to this would be almost seamless for a single ship; everything that ship needs would be self-contained in such a system. However, these types of services would not alleviate the requirement for a data-bearer amongst ships to enable the concept of a tactical cloud in a task group at sea.

11. Both government and industry have shown that they are highly motivated to see next generation wireless technology succeed. The recent announcement of the Evolution of Networked Services through a Corridor in Québec and Ontario for Research and Innovation (ENCOR) between five major telecom companies and the governments of Ontario, Quebec, and Canada is evidence of this.[12] Industry is eager to exploit this technology and the RCN is well positioned to benefit from this eagerness. The RCN is uniquely positioned to serve as a mobile proof of concept platform and work with the right industry partners in Canada to deliver these types of enabling capabilities that would support the concept of a tactical cloud at sea. Additionally, both dockyards could be outfitted with this type of technology to allow for wireless synchronization as ships return to home port. It goes without saying that the introduction of this type of technology would need to comply with, and be supported by, a significant number of policies and regulations which will be looked at in the following section.

Security Concerns and Government Policy

[12] Evolution of Networked Services through a Corridor in Quebec and Ontario for Research and Innovation (ENCQOR).“About ENCQOR.” Last accessed 13 October 2018.https://ontario.encqor.ca/about/

12. The growing demand for cloud computing services was anticipated by the government, which issued an IT Security Bulletin as early as 2014.[13] This document aimed to socialize some of the less understood risks about cloud computing such as data loss, lack of confidentiality and potential legal concerns about exactly where the data was being stored. More recently, the GC has issued updated strategy through the Communications Security Establishment (CSE) that will serve to guide departments when choosing cloud service providers.[14] In essence, this strategy incorporates a list of pre-qualified providers that have been vetted by Shared Services Canada (SSC) and meet specific security requirements. Both of these are practical and reasonable steps taken by the GC in an effort to embrace innovation while remaining cognizant of the potential security concerns that are inherent with any type of IT project. In a February 2018 Backgrounder, the GC indicated that more than 20 cloud computing contracts had been awarded through SSC,[15] which is a very promising indicator of the healthy appetite for cloud computing within the Public Service. This same backgrounder also noted that the "…first set of cloud services will handle unclassified data only."[16] This is also a promising sign, as it does not rule out the possibility that future cloud services may expand to cover classified material.

13. The framework established by the GC through SSC with the establishment of a vetted list of providers has created an environment that the RCN can benefit from. The implementation of a service contract with one of the pre-qualified vendors should be relatively swift in comparison to a capital program which could take years. Any solution that is pursued must be able to ingest data from the ship's organic sensors, the *Cyclone*, and any future advanced sensors like the RCN

[13] Communications Security Establishment. "Security Considerations for the Contracting of Public Cloud Computing Services." Last accessed 13 October 2018. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb-105-eng.pdf

[14] Communications Security Establishment. "Cloud Security for the Government of Canada." Last accessed 13 October 2018. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itse.50.060-eng.pdf

[15] Shared Services Canada. "Cloud Computing." Last accessed 13 October 2018. https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html

[16] *Ibid*

ISTAR UAS and MRB. The current restriction of unclassified data should not be used as an excuse to not pursue the implementation of this type of solution. If required, any classified data that was collected, such as signals intelligence, could be segregated and not stored on the tactical cloud. However, the remainder of the data collected should remain unclassified until some level of analysis has been conducted and then designated appropriately. Regardless, appropriate implementation of an unclassified cloud could then serve as a use-case and test bed to make the case to SSC for raising the acceptable classification level if necessary. The environment is permissive, the technology is available, and the RCN requires this type of tool in the fleet to adequately manage and exploit big data.

CONCLUSION

14. This paper set out to demonstrate how cloud computing could provide practical IT infrastructure to manage the imminent arrival of big data into the RCN fleet. The reality facing the RCN is that the ability to collect data through various sensors has outstripped the capacity to process or transfer that data in a timely manner. Future projects and sensors will only exacerbate this problem. Industry partners have developed solutions that seem to fit the unique operating environment faced by the RCN. These solutions would increase both the storage capacity and analytic processing at the edge. Finally, the GC has created an environment which fosters both innovation and the adoption of cloud-based technology. The RCN is well positioned to leverage both the potential for innovation in the communications networks sector as well as engage SSC to determine an appropriately qualified cloud-based service provider. Cloud-based computing is undeniably on the horizon for the RCN and that horizon is much closer than anticipated; it’s here now.

RECOMMENDATIONS

15. It is recommended that the RCN investigate the feasibility of employing a concept similar to the tactical cloud onboard the *Halifax*-class frigates through the use of a SSC qualified cloud service provider.

16. It is further recommended that the RCN also investigate the feasibility of conducting a proof of concept trial with an industry partner to determine the effectiveness of a next-generation network in transferring vast amounts of data throughout a task group.

BIBLIOGRAPHY

Amazon Web Services. "AWS Snowball Edge." Last accessed 13 October 2018. https://aws.amazon.com/snowball-edge/

Canada. Department of National Defence. *Leadmark 2050: Canada in a New Maritime World*. Ottawa: DND Canada, 2015.

Canada. Department of National Defence. *Royal Canadian Navy Strategic Plan 2017- 2022.* Ottawa: DND Canada, 2017.

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: National Defence, 2017.

Communications Security Establishment. "Cloud Security for the Government of Canada." Last accessed 13 October 2018. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itse.50.060-eng.pdf

Communications Security Establishment. "Security Considerations for the Contracting of Public Cloud Computing Services." Last accessed 13 October 2018. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb-105-eng.pdf

Department of National Defence. "Defence Capabilities Blueprint." Last accessed 13 October 2018. http://dgpaapp.forces.gc.ca/en/defence-capabilities blueprint/index.asp

Evolution of Networked Services through a Corridor in Quebec and Ontario for Research and Innovation (ENCQOR). "About ENCQOR." Last accessed 13 October 2018. https://ontario.encqor.ca/about/

Forbes. "The Top 5 Cloud-Computing Vendors: #1 Microsoft, #2 Amazon, #3 IBM, #4 Salesforce, #5 SAP. Last modified 7 November 2017. https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing vendors-1-microsoft-2-amazon-3-ibm-4-salesforce-5-sap/#3a2d3b426f2e

IBM. "Big Data Analytics." Last accessed 13 October 2018. https://www.ibm.com/analytics/hadoop/big-data-analytics

KPMG. "Journey to the cloud. The Creative CIO Agenda". Last accessed 13 October 2018. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/the-creative cios-agenda-journey-to-cloud.PDF

Microsoft Azure. "Azure Stack: An extension of Azure". Last accessed 13 October 2018. https://azure.microsoft.com/en-us/resources/azure-stack-an-extension-of-azure/

Porche III, Isaac R., Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney and Evan Saltzman. *data_flood Helping the Navy Address the Rising Tide of Sensor Information.* Santa Monica: RAND Corporation, 2014.

Shared Services Canada. “Cloud Computing.” Last accessed 13 October 2018. https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html

United States. Department of the Navy. *Maritime ISR Enterprise Acquisition (MIEA) Review*. Washington, DC: U.S. Government Printing Office, 2011. Last accessed 13 October 2018. http://pmatllc.com/whitepapers/MIEA_WhitePaper_FINAL_Signed.pdf

Wilson, Bradley, Isaac R. Porche III, Mel Eisman, Michael Nixon, Shane Tierney, John M. Yurchak, Kim Kendall, James Dryden and Sean Critelli. *Maritime Tactical Command and Control Analysis of Alternatives.* Santa Monica: RAND Corporation, 2016.