Cloud Concerns

Part 2

by LtCol C. Neil Fitzpatrick, USMC(Ret)

Cloud is the shiniest of the shiny new objects on the technology market. Many commercial firms have recognized the power of the cloud and leapt at the opportunities it offers; some have fully migrated. To a lesser degree the Federal Government, the DOD, and, specifically, the Marine Corps have been wary of the sparkle. While the DOD and the Marine Corps have provided approval for cloud migration through policy, there are legitimate concerns related to offloading services and capabilities to a cloud computing environment and especially to a commercial cloud environment run by contractors—a concept that conjures anxiety for many reflecting on the Navy Marine Corps Intranet (NMCI) project of the early 2000s. Comparing a modern commercial cloud to NMCI, however, is like comparing the F-35 Joint Strike Fighter to a Vietnam era F-4 Phantom. Both are military aircraft using jet technology, but that is about as close of a comparison that can be drawn. Nevertheless, concerns about adopting the use of a commercial cloud should be addressed. The benefits of a hyper-scaled commercial cloud far outweigh the disadvantages, and there are no concerns sufficient to prevent the Marine Corps from conducting a movement to contact with commercial cloud offerings through DOD approved cloud service providers (CSP).

Vulnerabilities and other security concerns. Security concerns have always been a trump card when evaluating new technologies. Historically and unfortunately, some security professionals have slowed the speed of advancement and have even had the power to prevent the movement to new technologies altogether. System and information security are essential to military operations, but security should be done with the attitude of enablement vice prevention. I can almost hear the security professionals gasping for air and see them shaking their heads. However, at high levels within the DOD, the relationship between security and operations relative to the cloud is changing:

> While security concerns were a traditional obstacle to increased adoption, there have been substantial advancements over the past two years as CSPs have been approved and used for sensitive workloads throughout the government—including the Defense Department … Security issues no longer dominate most of the meetings with knowledgeable senior defense officials.[1]

The U.S. intelligence community has been using the commercial cloud for years. As early as 2013, the CIA has been leveraging the Amazon Web Services (AWS) to develop a secret private cloud to support seventeen agencies within the intelligence community. Though they would not admit it at the time, two years later in 2015, the CIA broke their silence at an AWS Government, Education, and Nonprofits Symposium in Washington, DC. "This is an opportunity to refactor, reform and revitalize whatever you were doing in the past," said Alex Voultepsis, chief of the National Security Agency's Engineering and Planning Office for the Intelligence Community Special Operations Group.[2] During a panel conversation, he said that the Commercial Cloud Services cloud "has helped many agencies 'stuck in heritage systems' begin to phase those systems out in favor of using the [cloud]."[3]

Seven years ago, eminent U.S. intelligence organizations recognized that commercial cloud technology was secure enough for at least some of their operations, but many within the Marine Corps still harbor grave concerns that a commercial platform is riddled with vulnerabilities. On 6 March 2017, the DOD released version one, release three, of its *Cloud Computing Security Requirements Guide*, which details the security requirements necessary for the DOD to use commercial CSPs. The DOD has paved the way for this adoption. Their most recent contract award of Joint Enterprise Defense Infrastructure (JEDI) to Microsoft Corporation in October 2019 ushers in a new era of government IT collaboration with the commercial world. Security controls offered by commercial CSPs, such as Microsoft and AWS, include a shared responsibility model between the CSP and the customer, employing strong encryption of data in flight and at rest, third-party assessment organizations, the ability to leverage dedicated dark fiber networks, auditing and logging, user/administrator authentication, virtual private networks, virtual private clouds on dedicated hardware allocated to a single customer, and even organized and coordinated penetration testing on CSP platforms.

Another security concern proffered by traditionalists is that CSP customers are re-entering Pearl Harbor, where a large portion of military data assets are located in one port and subject to a single devastating attack. This argument implies a less-than-full understanding of how robust a commercial cloud can be. In a cloud, organizational data and

>LtCol Fitzpatrick was an 0602 Communications Officer and an 8825 Modeling and Simulation Officer. His last billet was as the IIMEF Operations Officer. He is currently the Senior Knowledge Manager at the DOD Information Analysis Center.

Marines must be able to operation in austere environments. *(Photo by Cpl Brennon Taylor.)*

services do not necessarily reside in a single location, though it can if that is the customer preference. With good infrastructure design and the deployment of cloud services, Marines can leverage a virtual private cloud that uses elastic load balancing to direct requests for resources among scores of data centers throughout the world. Major commercial CSPs designed their cloud infrastructure with this in mind by dedicating some domestic data center locations to the Federal Government and four specifically to the DOD. In addition to clouded military data being located where it is quickly available to the user, the physical CSP hardware platforms supporting military operations can be placed into an architecture that is physically separate from other CSP users. Furthermore, commercial CSPs offer data durability solutions that can be integrated into provisioned services, spread-loaded across regions, and even, if engineered properly, stored on physical media like CDs, DVDs, or tapes to meet the archiving requirements of Marine Corps customers.

An expeditionary Marine Corps necessitates an expeditionary network. Marines operate in the most austere environments on earth, so how could a commercial CSP support them where there is no access to the Defense Information Systems Network (DISN)? Most large CSPs have the global footprint necessary to support global Marine Corps exercises and operations. Establishing access to DISN services is always preferred. Access would be established in much the same manner as it always has been; echelon Marines from communications battalion/squadron transmission sections arrive on-site and immediately set up access via their long-haul/satellite communications equipment. There may be some occasions when DISN access is not possible for a time because of a delay in the communications architecture setup, weather conditions, or some other unforeseen circumstance. AWS offers a device called Snowball Edge[4] that connects to the deployed network and extends some key cloud services to the deployed environment that are resident on the main cloud. The Snowball Edge offers up to petabytes of portable data and may also act as a failover at a later time if DISN access is severed for some reason. This device is ruggedized and offers AES-256 encrypted storage capacity in a form factor about the size of a large desktop computing tower. The Microsoft offering is called Azure Stack, a similar concept built on Dell, HP, and Cisco equipment. Azure Stack provides infrastructure as a service (IaaS) and platform as a service for computing in remote environments.[5] Once DISN access is restored, the AWS and Microsoft devices can be configured to synchronize with the cloud to ensure data integrity. For longer periods of limited network access, or when the exercise/operation concludes, Snowball Edge and Azure Stack can be shipped back to their closest vendors' data center, where the data can be uploaded, archived, and synchronized with the respective main-cloud environment.

The Marine Corps already has a cloud. The Marine Corps Enterprise Information Technology Services (MCEITS) at Kansas City, MO, may fit the definition of a cloud in the broadest sense, but it is more akin to an enterprise-hosting environment. Its capabilities fall short of the services that large commercial CSPs are able to offer. Gartner's Magic Quadrant for IaaS, released in July 2019, names Amazon, Microsoft, and Google as the industry leaders for commercial CSPs, with all remaining providers only achieving the title of "niche players." Leaders provide the most complete vision and have the best ability to execute on that vision.[6]

MCEITS' final operational capability was in fiscal year 2014. By comparison, AWS achieved final operational capability in 2006, a full eight years prior to MCEITS, and has been adding additional capability ever since. By all practical measures, MCEITS provides niche services to the Marine Corps, but is not in the same class as those cloud offerings evaluated by Gartner and included in its magic quadrant assessments.

Access to the MCEITS environment is also tightly controlled, and configuration management is a laborious, time-consuming process. It is too slow and unresponsive to accommodate Marine Corps units' needs, especially when required during short-lived exercises and operations. Commercial CSPs like AWS and Microsoft provide a hyperscaled global environment that allows their customers to increase capacity instantaneously and to whatever level is required. Customers can modify their service configurations via a dashboard in realtime without going through the days- or weeks-long change management process required by MCEITS. In terms of services offered, MCEITS is

Some equipment may be vendor lock in. *(Photo by Cpl Brennon Taylor.)*

nowhere close to commercial providers. If not MCEITS, are there other DOD entities that offer cloud services that the Marines could leverage? There are. The DOD Information Systems Administration (DISA) milCloud and milCloud Plus are

> cloud-services product portfolio, managed by DISA, that features an integrated suite of capabilities designed to drive agility into the development, deployment, and maintenance of secure DoD applications. One of milCloud's core products is an [IaaS] solution that leverages a combination of mature commercial off-the-shelf and government-developed technology to deliver cloud services tailored to needs of the DoD. milCloud offers a managed hosting service called milCloud Plus, which provides implementation and hosting support services for DISA mission partners.[8]

DISA has completed the next generation to milCloud Plus, called milCloud 2.0. In milCloud 2.0, DISA authorizes connections to commercial CSPs, which is a recognition of the power of the commercial market. Furthermore, the DOD awarded a new cloud acquisition project in October 2019 called the Joint Enterprise Defense Infrastructure (JEDI), to Microsoft for $10 Billion over ten years. In terms of the amount alone, the DOD recognizes the power of the commercial market. The Marine Corps will inevitably continue to use MCEITS, but will likely use it less and less as JEDI services become more available and better understood.

Vendor Lock-In. Historically, there have been many programs and projects where the government contracts with a single vendor for a specialized product or service. Major aviation programs do this, but so do IT program managers. An example is limiting network equipment manufacturers to a minimum so that Marines do not have to learn a large number of operating systems and proprietary commands to make the network function. Cisco routing is a standard in the Marine Corps, as are the Microsoft desktop/server operating systems. Is this vendor lock-in? Yes, but it balances reliance on a single vendor against a standardized and commonly understood set of systems. A single set of tools that manage Marine Corps network and information resources also reduces the required number of standards that Marines must manage facilitating training efficiencies throughout the enterprise. Leading commercial CSPs offer easy solutions for the migration of data into and out of the cloud, where on-premises infrastructure is inelastic. Microsoft Azure, which is the infrastructure on which JEDI resides, offers import and export services to and from their data centers. This allows customers to try Azure and move their data out if they do not like it. Furthermore, this easy migration strategy reduces barriers to commercial CSP adoption and eases the minds of those concerned about vendor lock-in.

Business Case. Under the traditional acquisition model, the Marine Corps decides upfront how much capacity it requires and planners create a detailed equipment string; purchase the required equipment; carve out precious physical space within buildings to house it, power it, and cool it; and dedicate a team of personnel to install, configure, and maintain it. When this effort is finally completed, years have passed, the equipment is several years old, potentially millions of dollars have been spent, and the Marine Corps has received exactly zero return on investment. Infrastructure investments are upfront sunk costs and are made prior to these networked capabilities delivering their service to the customer. Avoiding these sunk costs is a major advantage of the commercial cloud offerings via IaaS. Most hyperscaled CSPs leverage a pay-as-you-go model. Commercial CSPs incur all of the infrastructure investment costs. They then make them available and ready for use at the exact time the Marine Corps needs them. Pay-as-you-go is already being leveraged by other federal agencies. They "can turn [it] on and off with the click of a button, and only pay for what they use."[11] Commercial CSPs do not require minimum spend commitments or long-term contracts, unlike the NMCI of the early 2000s. With modern cloud services and like electricity or water, the Marine Corps gets all that it wants and pays for no more than it uses.

Marine Corps MOSs do not include training for cloud services. The same expertise that the 06XX community currently possesses will still be used to provide the Marine Corps with network and IT services when there is a significant move to a commercial CSP. Some future MOS balancing may be necessary as the Service shifts from a do-it-all-yourself mindset to sharing responsibility with CSP partners, but this could be phased in over time. Ma-

Some MOSs don't include training for cloud services. *(Photo by LCpl Kaleb Martin.)*

rines currently use their training and skills to work on a set of physical and virtual servers located in a centralized data center within a hardened building or within a tent in the field. Their function in a future communications environment using a CSP will not be that different. Marines will still provision compute and storage resources and build out their own network capabilities within the cloud. A future cloud model would balance the location of resources between on- and off-site vice one operated and maintained exclusively by the Marine Corps.

Marine Corps culture. Marines can do anything, but they cannot do everything. There has always been the attitude within the Marine Corps that we do it better. The pace for the development of new technology is happening so quickly that Marine Corps acquisitions has not been able to keep up. For many years, Marine Corps IT services have been in a never-ending cycle of plan, procure, and maintain until the equipment is sent to the Defense Reutilization Management Office to remove it from the operational inventory. The Marine Corps should now consider off-loading the burden of keeping up with the latest and greatest technology to a commercial cloud partner, a fact recognized in the recent JEDI award Allow the CSP to procure and patch the servers. The Marine Corps will train Marines to best leverage the cloud and avoid trying to build a network from scratch each time a network is required. There is no doubt that the commercial IT sector's ability to deliver the most advanced modern hardware/software resources and cloud services to customers is better than the Marine Corps' or even DISA's ability to do so.

When considering a decision to migrate some services to commercial CSPs, there are plenty of legitimate concerns. The Marine Corps cannot afford, however, to plod slowly forward improving its communications and IT infrastructure at the glacial pace of traditional acquisitions. Non-state enemies do not build data centers, provision physical servers, or install fiber networks themselves; they leveraged mobility based on global access to commercial networks and services built and operated by the commercial IT sector. Achieving a decisive advantage cannot be accomplished by nibbling around the edge of the new technology pie. Like LtCol Pete Ellis' bold and disruptive 1920s vision of the future, we must now look deeply into ours and recognize that the IT tactics, techniques, and procedures of yesterday are a dead end. The Marine Corps, especially smaller tactical units, must evaluate, test, and implement new commercial cloud technologies immediately to achieve and maintain a clear IT advantage in the information and knowledge age of the 21st century.

Notes

1. Jennifer Chronis, "The Untapped Potential of the Hyperscale Cloud," *National Defense*, (Arlington, VA: March 2017).

2. Frank Konkel, "What do US Intelligence Agencies and Netflix Have in Common? Both are Amazon Cloud Customers," *Nextgov*, (Washington, DC: June 2015).

3. Ibid.

4. "AWS Snowball Edge Features," *Amazon Web Services*, available at https://aws.amazon.com.

5. "Hybrid Application Innovation with Azure and Azure Stack," *Microsoft*, (March 2017), available at https://go.microsoft.com.

6. Raj Bala, Bob Gill, Dennis Smith, and David Wright, "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide," *Gartner*, (July 2019), available at https://www.gartner.com.

7. Mark Coppock, "Microsoft is a Leader in 18 Gartner Magic Quadrants, Including Cloud Infrastructure as a Service," *On Mfst*, (August 2016), available at http://www.onmsft.com.

8. "milCloud Plus," *Defense Information Systems Agency*, (Washington, DC: January 2020).

9. Lauren C. Williams, "DOD Details its Plans for JEDI Cloud Contract," *Federal Computer Week*, (March 2018), available at https://fcw.com.

10. Bob Tuohy, "Advancing Threats Necessitate New Approach to Defense Technology Acquisition," *NextGov*, (June 2018), available at https://www.nextgov.com.

11. "The Untapped Potential of the Hyperscale Cloud."