Into the Clouds

Part I

by LtCol C. Neil Fitzpatrick, USMC(Ret)

>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.

One does not have to be Pete Ellis to recognize that Marines will continue to operate in all warfighting domains. Cyber is unique in the sense that it intersects and binds together each of the others. Through LtCol Pete Ellis' pursuit of military studies, extensive travels, and strategic and tactical analyses, a vision of a new "role for the Marine Corps as a mighty amphibious force" emerged twenty years prior to becoming necessary to defend against the aggression of the enemies of the United States.[1] LtCol Ellis precisely predicted an antagonistic Japanese Empire, complete with a plan of attack and warfighting equipment that did not even exist at the time. His prophetic and disruptive vision prompted a change in the role and mission of the Marine Corps, culminating in the development of the Corps' amphibious warfare doctrine. This new doctrine drove acquisitions, planning, and training for decades and continues to influence many decisions of the 21st century Marine Corps.

Such strategic vision has not been absent in the modern assessment of fighting in the cyber domain, but concepts of network and information technology (IT) support are still very much rooted in ideas and strategies developed decades ago. Marines are still trained to plan, install, operate, and maintain (PIOM) tactical network infrastructures from the ground up. Because of the expeditionary nature of the Corps' operations, to some degree, this will always be required. However, the enormity of this task should not be misunderstood. To PIOM its own garrison networks, Marine Corps personnel must maintain large secure facilities with consistently clean power, enormous cooling systems, and a fleet of support personnel (Marines, civilians, and contractors) just to keep the systems online. Beside the transmission systems and network infrastructure, the many services hosted by Marine Corps data centers require extensive expertise to maintain virtualized stacks of servers, operating systems, and scores of resident client/server applications. After the physical planning and installation of IT equipment and services, the meticulous phase of maintenance begins, in which a steady stream of security patches is applied across every single layer of the system. This is a continuous, never-ending task. Even though some of this process is automated, it is still extremely time consuming for network and IT support personnel to scan and maintain an enterprise of IT resources. This historical model is no longer serving the best interest of the Corps. The Service must be able to quickly plan, test, and establish baseline tactics, techniques, and procedures (TTP) to transition at least its sensitive-but-unclassified network and IT services to a commercial cloud service provider (CSP) or risk being outpaced by its adversaries.

In the 1920s, the idea that the Marine Corps would spearhead an amphibious island-hopping campaign in response to an act of war by Japan was unthinkably disruptive. Until recently, the notion that the Marine Corps should need to migrate most of its network and IT services to a commercial cloud has been equally disruptive. This is because there has been no critically compelling reason to do so. Disruption means challenging conventions and even criticizing time-honored and historically successful strategies. Disruption creates chaos for a time until it can be fully integrated into the fabric of the organizational thought. Incremental technological change is safer and less uncomfortable, but it takes far too long to bring needed innovation to the warfighter. Other DOD services are disrupting historical norms and aggressively adopting cloud services in various forms. As far back as January 2017, the Chief Technology Officer for the Air Force said,

> We're going to outsource all that capacity and data centers at the base level … We do not have enough airmen to actually do the jobs … That's not their mission in life.[2]

Sound familiar? The Marine Corps is not the Air Force, but both Services share many similarities regarding base infrastructure and the operation and maintenance of deployable networks. In recognition of this need to modernize, on 25 October 2019 the DOD awarded the Joint Enterprise Defense Infrastructure (JEDI) cloud contract to Microsoft Corporation, a contract work $10 billion over the next ten years. However, to arrive at an award, the DOD acquisition process still took several years to accomplish. Now that it is finally in place, the contract will facilitate a migration from traditional IT infrastructures and facilitate enterprise level Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) capabilities.

Striking the right balance between speed and the thoroughness of IT acquisition is a dilemma. During the traditional lengthy period of incremental technological improvement, the adversaries of the United States outpace us by using the best the commercial world has had to offer, such as social media and commercial cloud services. Without the disruptive vision of Ellis and actions of the Marine Corps' leadership of the 1930s, the force that won the Pacific would have still been guarding naval bases and not even thinking about an advanced amphibious assault campaign against the Japanese empire. An unwillingness to embrace and subsequently implement disruptive IT capabilities has limited the Marine Corps' speed and agility in leveraging advantageous commercial cloud technologies. Not only is it vital to have the tools and capability present to conduct a migration to the cloud, the service must ensure policy is present and there are incentives to do so. The DoD Cloud Strategy (December 2018)[3] and the Marine Corps' Deputy Commandant for Information Memorandum entitled, *Modernization for Cloud Policy* (May 2019)[4] have cleared the path for migration. Now units and bases must get serious and do it.

Modern adversaries of the United States adopted advanced commercial cloud communication technologies years ago. They understood that the level of sophistication and power contained within these applications and systems go well beyond that which they could create themselves. They were not constrained by a years-long acquisition process and moved quickly toward the advanced technological paradigm. According to a July 2016 article by CNBC writer Harriet Taylor, entitled "Islamic State's Favorite Technologies Outlined by Study," cloud technologies and encryption had become a standard within the terrorist group because they (the technology present with a commercial cloud) are effective at distributing their message and can be used anonymously.[5] Few deny that commercial technology is the direction in which the Marine Corps must transition to increase its IT advantage. Continuing to rely on traditional communication TTPs and acquisitions is too slow, and most senior military leaders freely admit to this. In most cases, though, the military acquisition mechanisms in place have not changed and Marines still deploy technology to the field in only incrementally more advanced ways than it did a decade ago. The commercial Internet-based nature of cloud services and their pricing models turn the traditional operational concept of military IT communications upside down.

Under current communications and IT paradigms, Marines must maintain the expertise to support a growing number of hardware and software products that continue to increase in complexity and interdependency. The military relies on the commercial industry to develop security patches and determine when and where they should be installed. In most cases, cyber TTP are already drawn directly from companies such as Microsoft, Cisco, and the numerous other vendors that provide hardware and software to the Marine Corps. Generally, the vast majority of Marines do not have the technical expertise to validate all cyber TTP and patches developed by commercial vendors and, therefore, rely on a trust relationship with them. This is an acceptable risk because it allows for a good division of labor between the Marines and their commercial partners. Each organization should be able to concentrate on core competencies while maintaining an awareness of other important mission areas. This is the construct that produces the best possible outcomes, balancing cyber operations with cyber security. The challenge for the military mind is the adoption of commercial cloud technologies.

The Federal Government has been using commercial cloud services for years,[6] but aggressive cloud adoption arguments within the Marine Corps continue to be met with the proverbial cyber security trump card. Statements such as, "it's too risky," "unproved," and "not applicable to the expeditionary mission of the Marine" are tired and worn. The DOD Chief Information Officer and the Defense Information Systems Agency co-published the *Cloud Computing Security Requirements Guide* (CCSRG) in January 2015. The document clearly states that it intends to facilitate DOD cloud strategies and comply with DOD IT security requirements to increase mission effectiveness:

> Cloud computing technology and services provide the Department of Defense (DoD) with the opportunity to deploy an Enterprise Cloud Environment aligned with Federal Department-wide Information Technology (IT) strategies and efficiency initiatives … Cloud computing enables the department to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. The overall success of these initiatives depends upon well executed security requirements, defined and understood by both DoD Components and industry. Consistent implementation and operation of these requirements assures mission execution, provides sensitive data protection, increases mission effectiveness, and ultimately results in the outcomes and operational efficiencies the DoD seeks.

The CCSRG specifically authorizes the use of "Commercial and non-DOD Federal Government CSPs."[7]

In deployed environments, it is mission critical for the Marine Corps to get network and IT services established as quickly as possible. When communications Marines deploy forward, they arrive on site and turn to a number of essential but time-consuming tasks. They establish satellite access as a gateway back to the Defense Information Systems Network and simultaneously install operating systems and configure software on tactical servers, create accounts for network access, and apply patches to prepare for the arrival of the main body. This can take weeks even if some of this was accomplished prior to the actual deployment. This is both too slow and too labor intensive.

The commercial cloud is ever present and has one key requirement: access to the Internet. Once forward deployed Marines establish access, they can offer their users an environment where software is already installed, accounts have already been created and are ready for use, and all security patches have been tested and validated, even those that were released during the Marines' transition to the remote location. Marine Corps requirements, such as security, worldwide availability, access to existing command and control capabilities, agility, mobility, and scalability are already provided by commercial CSPs. This relationship allows Marine Corps IT to keep current with the latest commercial technological advancements while shifting the burden of lower-level network and patch management away from unit communicators. By reducing this maintenance overhead, communicators do not abdicate their role for providing network and IT services to the command. Instead, their role shifts from managing local hardware and software, replete with maintenance and configuration challenges, to managing a commercial cloud instance that focuses on offering immediate capability to a commander.

Innovative modern commercial cloud technology may be used now throughout the Marine Corps because PIOM can be accomplished in a way that exactly replicates the traditional Marine Corps production network configuration. Amazon Web Services, one of the well-known commercial CSPs, complies with Federal Government cloud policy and maintains an isolated region to host sensitive DOD data and regulated workloads in the cloud. These capabilities:

- Meet the Government security standards of the Federal Risk and Authorization Management Program, a Federal "government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services,"[8] International Traffic and Arms Regulation, CCSRG levels one through four, Health Insurance Portability and Accountability Act, and more.
- Offer a set of constantly expanding features.
- Deliver economy of scale and consistently lower costs, auto-scaling to reduce the need to constant capacity planning, eleven 9s of availability (i.e., 99.999999999%), massive reduction in data canter costs, and the integration of a tactical service-oriented architecture.

Amazon, Microsoft, and other industry leaders in commercial cloud offerings present a rich menu of capabilities to DOD customers. They have already built massive capacity and are capable of meeting Marine Corps network and IT service requirements for unclassified-but-sensitive data and even some levels of classified networks. Capabilities include provisioning the following services/capabilities:

- Computing power and networking. Auto-scaling.
  - Elastic load balancing.
  - Virtual private networks between the government site and the CSP.
- Storage.
  - Any amount required.
  - Archiving and online backup.
  - Massive scale data import/export/transport solution to and from the CSP.
- Database.
  - Fully managed high-performance relational database services.
  - Petabyte-scale data warehouse service.
- Analytics through artificial intelligence and machine learning
- Organizational configuration and management tools.
- Security.
  - Access control.
  - Logging.
  - Contractual and regulatory compliance management.
  - Resource and application monitoring.
  - Application Services.
  - Messaging.
  - Workflow service for application development.[9]

Prior to the October 2019 award of JEDI, DOD services had the flexibility to acquire and test commercial cloud services from a number of vendors, as long as they complied with standard DOD security regulations. Now that JEDI has been awarded to Microsoft and many existing services are in the midst of migration, it makes less sense to acquire services from anyone else. JEDI advertises a full complement of cloud-based services, which would enable the Marine Corps to simply choose the capabilities it wants from a menu and manage them via the CSP's management console, paying for only the services, storage, and bandwidth it uses. Security in the cloud and of the cloud are concepts that must be clearly defined early as units begin to migrate to JEDI. The cloud security model is one that is shared between management of the infrastructure and management of the software. These capabilities are no longer some future concept yet to be developed; they are available, fully functional today, and consistently advancing. Commercial cloud technologies represent the greatest untapped resource for the Marine Corps in the modern technological era. One does not have to have Pete Ellis' vision to see that a resistance or slow migration toward the commercial cloud creates a technological offset in favor of our adversaries that could result in detrimental consequences for approaching Marine Corps missions.

Notes

[1] Col David H. Wagner, "The Destiny of Pete Ellis," *Marine Corps Gazette*, (Quantico, VA: June 1976).

[2] Frank Konkel, "Air Force CTO: We Don't Want To Manage IT Anymore," *NextGov Emerging Tech Blog*, (January 2016), available at http://www.nextgov.com.

[3] Patrick M. Shanahan, DoD Cloud Strategy, (December 2018).

[4] Marine Corps Deputy Commandant for Information, *Memorandum: Modernization for Cloud Policy*, (Washington, DC: May 2019).

[5] Harriet Taylor, "Islamic State's Favorite Technologies Outlined by Study," *CNBC*, (July 2016), available at http://www.cnbc.com.

[6] Sydney J. Freedburg, "Making the Cloud Work for the Military," *Breaking Defense*, (September 2014), available at http://breakingdefense.com.

[7] Defense Information Systems Agency, *Department of Defense Commercial Cloud Security Requirements Guide*, (Washington, DC: January 2015).

[8] "About Us," *Federal Risk Authorization Management Program*, available at https://www.fedramp.gov.

[9] "AWS GovCloud (US)," *Amazon Web Services*, available at https://aws.amazon.com.