The Challenge and Opportunities of Standing on Cloud – Finding our Warfighting Advantage

Rear Admiral Danelle Barrett
Andrew Mansfield

The Navy is dealing with the challenges of a world where exponentially accelerating and converging technologies impact the way we operate at unprecedented speeds. We must quickly leverage the operational advantages emerging technologies bring to warfighting and be forward-leaning in disrupting their use by adversaries. Similarly to how cloud technologies and Smartphones have fundamentally changed the way we live by accessing and using information in revolutionary ways, victory in warfighting will go to those forces with similar information supremacy. Cloud technologies provide an opportunity to achieve that supremacy, enabling extraordinary benefits through scalable services which support Big Data analytics, Artificial Intelligence (AI), and machine learning. Transition away from stove-piped capabilities and sources of data to a cloud environment where authoritative data can be exposed, discovered, and shared for improved situational awareness and decision making is the future. However, the move to the cloud does not come without risks and challenges.

Naval operators must understand the risk of data in the cloud and ensure appropriate oversight of our information in the new cloud environment. Provisioning cloud to the tactical edge also poses challenges: synchronizing data between ashore and afloat, and moving information in the most efficient, secure, and operationally relevant manner. Finally, while cloud technology presents opportunities, the most significant challenges will be human. Cultural barriers to sharing information and training the Navy force to think about information in a new way must be addressed. Humans and machines will combine to define the context of data to become self-aware, self-learning and act predictively, doing the heavy lifting to correlate and use information at a speed and level of complexity our brains are incapable of today. There are no bystanders in this effort. It will take all hands in active engagement to understand the tools at our disposal and use them to achieve unparalleled warfighting effects.

Rear Adm. Danelle Barrett graduated from Boston University in 1989 with a Bachelor of Arts in History. She holds Master of Arts degrees in Management, National Security/Strategic Studies, Human Resources Development and a Master of Science in Information Management.

Her operational assignments include tours at U.S. Naval Forces Central Command/U.S. 5th Fleet; 2nd Fleet, Carrier Strike Group 2, Multi-National Forces Iraq, Carrier Strike Group 12, with deployments supporting Operations Enduring Freedom in Afghanistan and Unified Response in Haiti; and deputy director of current operations at U.S. Cyber Command. Her multiple shore tours include commanding officer, Naval Computer and Telecommunications Area Master Station Atlantic; and chief of staff, Navy Information Forces Command.

Barrett currently serves as the Director of Navy Cyber Security.

Personal awards include Copernicus Awards 1998, 2000 and 2005; DoD Chief Information Officer Award, first place individual category 2006; Federal 100 2010; AFCEA Women in Leadership Award 2014; Women in Technology Leadership Award 2017. She has published 29 articles.

To understand how to use the cloud for operational warfighting lethality and improved efficiencies, it is important to understand what the cloud is. "Cloud" is the current buzzword of the day in strategy and marketing briefs, but it is hardly a catchphrase in practice. It is Information Technology (IT) delivered as a service to enable access to information from anywhere, at any time, and is not limited to specific machines or systems. Unlike traditional client/server architectures, it provides a platform to rapidly configure and expand resources and capabilities and enables orders of greater magnitude, speed, and agility to deploy and integrate that capability. Cloud facilitates improved cybersecurity of information through precise monitoring of access points to protect information from unauthorized use. The commercial industry has invested heavily in cloud research and development, and those technologies and services matured at unparalleled rates, a trend that is expected to accelerate. This can contribute to the confusion about what the cloud is. As cloud momentum in the commercial industry continues at breakneck speed, even the term cloud will morph as the next business and technical architecture replaces the cloud of today. The Navy needs to stay aligned with industry best practices and employment of the latest models so that we seamlessly transition and evolve our IT on pace with industry.

To understand cloud as a warfighting enabler, it's important to note cloud is not simply "someone else's computer." The reality is much more expansive as cloud design and capabilities cover the breadth of IT, from networks, hardware, computer management capabilities, and storage of data, software platforms, and the applications that ride upon them. Cloud is a way of looking at IT as a set of discrete, distributed, and malleable services and capabilities. Those capabilities are not tied to any specific piece of hardware, software or network. Industry has led an adherence

Andrew Mansfield is the Naval Information Warfare Center (NIWC), Atlantic Executive for Network Centric Development and Integration. He serves as the Technical Director of NIWC. He engages at a national level in charting the course for the Navy's IT modernization efforts, specializing in areas of commercial cloud/cloud transformation, Data Sciences and Analytics, and Cyber Security. Mr. Mansfield was appointed as an SL in October 2011 and has over 33 years of federal service. His contributions include: Serving as the 5.0 Engineering Lead/ Chief Engineer and as the national lead for Net-Centric System-of-Systems Engineering and Integration (SE&I). He led the modernization of the Veteran's Administration Chapter 33 GI Bill Benefits capability and was the National and Local Lead for the Command & Control (C2) and Business Information Technology (IT) Competency.

to open standards and cloud technologies have matured to a point where they are interoperable, widely available, and easily consumable.

Cloud means Navy content owners and application developers can now design, engineer, integrate, and continuously evolve each of these architectural elements in the cloud almost entirely independently from each other while still retaining overall integration and interoperability. It also makes the infrastructure agile and flexible enough to holistically adapt and scale up and down to the available capacity (i.e. network, processing, and data storage needs).

Cloud can be used to develop and execute offensive operations to deny adversaries access to their information at the time of our choosing. On a ship at sea or a tent in the desert, warfighters will manage the local hardware and software to access the cloud at the tactical edge, synchronized with a larger cloud ashore, allowing operators to be self-sustaining in a fight. Extending key portions of Navy cloud infrastructure to the tip of the spear will enable the Navy to employ the higher-level AI and machine learning to expedite command and control, operations, and improved decision making at the tactical edge. Cloud is necessary to enable next-generation technical capabilities such as Internet-of-Things (IoT), AI, Human-Machine Teaming, and Augmented Reality. By combining cloud computing with new warfighting Tactics, Techniques, and Procedures (TTPs), operators will have decision advantages and the ability to generate operational effects at the tactical edge not achievable with legacy IT infrastructure. This includes providing a platform for executing tactical cyber offensive and defensive effects. On the defensive cyber side, the flexibility of cloud technologies enables our ability to maneuver around adversaries' defenses while strengthening our defenses by minimizing disruptions.

From a cyber operations perspective, the unique capabilities of cloud computing can be applied in several ways. In the thick of battle, the warfighters can be limited by the information available, particularly with our dependence on satellites to reach back to shore. It is critical to have an end-to-end information platform that synchronizes our ashore and afloat cloud environments and to exchange data specific to that ship Commander's mission. Unlike current architectures where capabilities are typically tightly coupled to the hardware they're delivered with, cloud can maximize IT to its fullest extent. The ability to surge computational resources for high priority operational missions, including cyber offensive operations, could be prioritized and allocated quickly through automatic scaling by design. Cyber tool capabilities will be helped by computing capacity in a cloud environment and given priority access to infrastructure resources needed to execute operations. Cloud analytics have the potential to identify adversary network vulnerabilities at greater speed and precision, while simultaneously protecting our resources, making systems more resilient for fighting through attacks.

This rapid means of discovery and situational awareness of the adversary using cloud provides speed to effects. Cloud-enabled AI will aid cyber operators to see the cyber battlespace in near real-time, constructing and modeling ad-hoc capabilities for tactical warfighters to employ. For example, a team of Marines that is preparing to breach a building, having deployed from a littoral amphibious combat ship, could benefit from cloud-enabled AI. The building itself has security measures, locks, cameras, lights, etc. Unmanned platforms, working in conjunction with cyber tools and sensors are deployed. They quickly scan networks to build an initial view of the security systems and infrastructure in the building. This data is relayed back to the littoral platform and loaded into the tactical cloud for quick forensic analysis. Working in the tactical cloud and reaching back to greater cloud resources ashore when available, offensive cyber operators can create custom measures informed by the latest intelligence, test their assumptions on the tactical edge cloud, then load the cyber counterattack strike package on the deployed systems. Using the near real-time intelligence, the ground forces near the building receive constant updates and have accurate situational awareness of the environment to move with confidence around the battlespace. They know what devices are connected in the building and may even have sensors to provide visibility on combatants located inside. Should the adversary launch weapons to deny access to the cloud or strike platforms, advanced cloud network sensors could rapidly detect this activity and adapt by pre-emptively reconfiguring pre-approved counterattack strike packages and system defensive counter-measures to continue the attack. Data from the attack are used for trend analysis of adversary TTPs, building a repository of shared knowledge between all ships and back through the shore cloud to the Department of Defense (DoD) and other partners. While this sounds like science fiction, it is possible with today's technology, and cloud provides the needed capabilities to make it happen. Using the cloud for collaboration, AI, Big Data analytics, and to rapidly reconfigure resources to act and provide digital representation of an enemy system, gives cyber warriors at the tactical edge the platform they need to execute cyber operational effects.

Getting the cloud as a platform to the tactical edge to achieve this kind of warfighting advantage requires us to innovate how we provide our IT infrastructure afloat. In buying commercial cloud as a service from end-to-end, from the enterprise ashore to the tactical edge afloat, we must challenge all existing models in use for developing and delivering information capabilities. Under the Navy's "Compile to Combat in 24 Hours" initiative to transform the information environment across the enterprise, options are being explored for permanent commercial cloud services and infrastructure extended shipboard to replace government-owned infrastructure for processing, accessing, and displaying information. In this cloud infrastructure, shared servers, used by many application owners to host software code and data, would remain owned and maintained by the commercial vendor.

The Consolidated Afloat Network Enterprise Services (CANES) is the program that modernizes shipboard network hardware and software, and the shared computing environment described above represents "the brains" of CANES networks afloat in the government model. By modularizing the "brains" from the rest of the CANES infrastructure (routers, switches, workstations, etc.), the commercial vendor could modernize software elements instantaneously and update hardware more frequently to improve information processing. The vendor's tools, analytics, and improved cybersecurity capabilities would be purchased as part of the service, improving reliability and efficacy of information to support operations. They could also ensure synchronization of the afloat and ashore data clouds and enhance the quality of service by tagging and compressing data to move in a prioritized manner. This would get us to a level of information superiority that is not achievable with today's infrastructure, allowing operational commanders to get the right information at the right time.

All the benefits of using commercial vendors to provide cloud services come with risks and we must be deliberate in how we protect our information in the cloud. Even in that, however, there are advantages to cloud. Today, the Navy has myriad combinations of network hardware and software across the Navy enterprise that lack rigorous configuration management and pose an increased surface for cyberattack. Certainly, significant defense in depth investments were made over the last several years to build in resiliency and reduce our attack surface, but commercial cloud offers us opportunities to further improve this environment. Storing Navy information in the commercial cloud allows us to move at "industry speed" in employment of cybersecurity upgrades and processes, in addition to the other benefits of big data use outside the cybersecurity arena. Industry does not, however, have a long track record of decades of commercial cloud provisioning and it is prudent to fully understand how information will be protected in this new shared cloud responsibility model. The movement of Navy information to the commercial cloud must be executed in a deliberate manner with an understanding and acceptance of this risk and in comparison with the risk of continuing along the current path with its own significant cybersecurity challenges. Note that this is true in all our security domains. There will be separate cloud environment offerings for classified and unclassified information, provided by government and commercial industry.

Over the past year, the Navy has been working closely to define an initial model for "Command and Control" (C2) of Navy information in the commercial cloud. Specific actions must be performed to ensure C2 of our information in that environment that may be unique to how the Navy or DoD operates. For example, during a cybersecurity incident, a commercial vendor may be required to start an incident response. However, doing this may cause a loss of cyber activity situational awareness needed for other purposes. This requires collaboration with vendors, cybersecurity operators, and engineers to develop a detailed shared responsibility model, where cybersecurity tasks, data, and reporting requirements are well coordinated and implemented between government and industry. We are also ensuring we have standardized contracting language to enforce the requirements with our partners. Navy contracting language needs to provide for a decision window to approve moving forward for incident response or waiting while Navy cyber operators hunt an adversary. Acquisition professionals will ensure contracts are properly standardized for C2. Cyber operators and information owners can have the confidence to access the information when and where needed, and that lines of responsibility and accountability are well defined. As more partners enter the field, the model will continue to evolve.

This same model is needed across the DoD and so the Navy has shared this C2 construct with DoD teams working cloud contracts. Additionally, as the DoD and the Navy continue to harden their networks, adversaries increasingly look to softer targets to get at Navy information. There has been a significant increase in intrusions across industry to include Cleared Defense Contractors (CDCs) and their subcontractor networks to steal information. Options should be explored for CDCs and others who handle Navy information to store that in Navy commercial cloud environments where C2 can be properly executed, and we would have increased confidence in the cybersecurity of their data environment.

Making the cloud-enabled warfighting environment real is not just a technology challenge, it involves people, processes, and technology changes that are fundamentally transformational to how we operate today. We must prepare across all disciplines to embrace the capabilities enabled by cloud, adapting to this new IT ecosystem. Training should be integrated into all areas on how to manage, maintain, and operate on a cloud-driven information warfare platform.

The biggest challenges will not be technological. Fundamental changes in the culture of how we design, field, and deploy IT are needed, and cloud technology allows for an improved model over traditional IT deployment. This change includes networks afloat running AI at the tactical edge cloud to automatically reconfigure based on the operator need and responding and recovering from enemy attacks without a human in the loop. This highlights the increasing trust and confidence in machines' ability to make informed decisions with precision and speed.

Cloud is necessary to move the Navy to the next level of warfighting superiority, addressing challenges posed, particularly by near-peer competitors as defined in the National Defense Strategy. Our information warfare platform needs cloud and its benefits to ensure success across all warfighting lines. As our adversaries can buy the same capabilities, our dominance will depend upon our agility and innovation to quickly deploy cloud to achieve unmatched warfighting effects. As noted by the Chief of Naval Operations and other senior leaders, cyber and space will be where we see the battle beginning—and its end will hinge on the resilience, agility, speed, and flexibility with which we deploy cloud and capabilities which leverage them for our deployed forces.