Cloud Conundrum

Maj William Giannetti, USAFR

Last September, "Russian" cruise missiles were streaking toward the continental United States. Sophisticated cyber attacks against US interests overseas and laser-dazzling of reconnaissance satellites preceded the launch. At Joint Base Andrews, Maryland, the tracking data poured in real time, and operators across the country stood ready. It was the second in a series of on-ramps (or testbeds) for the Advanced Battle Management System (ABMS), a military Internet of Things that rapidly links data to decision-makers and provides commanders a menu of shooters.

BQM-167 target drones played the incoming cruise missiles, and the commanders made their selections. Over Creech Air Force Base (AFB), Nevada, an MQ-9 Reaper shot down one BQM-167 with an AIM-9X missile. An M-109 Paladin shattered another "cruise missile" in seconds at White Sands, New Mexico, with an experimental hypervelocity shell.[1] For the Joint Force, the display of firepower was a technological coup. "Tanks shooting down cruise missiles is awesome—video game, sci-fi awesome," said former Air Force acquisitions chief Dr. William Roper.[2]

Behind the scenes, classically stovepiped command-and-control data flowed at 5G speed. The Department of Defense's (DOD) array of "ONE" products supported mainly by public cloud mega-brokers Amazon Web Services (AWS) and Microsoft Azure made the linkages possible. OmniaONE, fed by dataONE's Unified Data Library, provided the on-ramp's "space to mud" common operating picture. For secure cloud applications, cloudONE provided remote data storage, and for war fighters, edgeONE did the same.[3] The on-ramp evidenced some impressive benefits, yet what are the risks of this military partnership with the public sector? History provides an answer.

The Cloud: A Brief History

According to the National Institute of Standards and Technology, a cloud is a ubiquitous, shared pool of configurable computing resources "that can be rapidly provisioned and released with minimal management effort or service provider interaction."[4] In short, a person uses someone else's computer—for a fee—to run their apps, process their data, and store their work. For almost a decade, AWS and Microsoft have dominated the public cloud market. Their storied competition for

the Joint Defense Enterprise Infrastructure (JEDI)—a "one cloud to rule them all"—has played out in court. They rent shared computing resources to customers inside their standard data centers, and there is extraordinarily little for the individual user to do. Patches and updates are done remotely, and interruptions are seldom.

Private clouds, on the other hand, are tailored for customers who have industry-specific or regulatory needs. Insurance companies, health management organizations, and investment firms typically use this type of cloud. The Defense Information Services Agency (DISA) offers private clouds to military customers with sensitive projects. The infrastructure is supervised inside the workplace or overseen off-premises inside a secure location. Like AWS and Azure, DISA offers an enterprise cloud, which is just a more expansive grouping of servers, routers, and switches. If a cyberattack happens in smaller, private clouds, defenders have less to focus on and more time to fight off a problem before it spreads.

But where did the cloud originate? Its founding concept precedes the internet as we know it. In the 1950s and 1960s, IBM's reel-to-reel mainframes employed a time-share model that allowed multiple users to use one computer. About this time, "mad" Major John Boyd, USAF, experimented with an IBM-704, testing an idea that influences combat aircraft's design and performance today—the energy-maneuverability theory.[5] The 1980s wave of computer resources' decentralization swept the old mainframes into the dustbin. Local ethernets codesigned by Bob Metcalfe linked single points of presence to businesses and industry.

Then, in 1996, two advertising men from Compaq—Sean O'Sullivan and George Favaloro—had an idea. Compaq servers were known for their reliability, and analysts projected $2 billion in sales to fledgling internet service providers like AOL. The duo looked at network engineering drawings, the wiring diagrams within them, and how a cloud signifies distant connections. A slogan was necessary—something that would make the company's products synonymous with the newly expanding internet. "Cloud computing" was born, though it did not become a household name until 2006. Google and Amazon began using the phrase to describe a new paradigm when people were accessing their software and computing power, not with their desktops but via the Web.[6]

The Value Proposition

A public cloud's value proposition is what buyers find most attractive. In essence, like any utility—water, electricity—you only pay for what you need. The mid-2000s saw growing interconnections between individuals and organizations that together made cloud computing economically attractive.[7]

The cloud industrialization push by AWS and Azure implies economies of scale, where average production cost falls as output volume increases.[8] At the dawn of the American Industrial Age, scale meant more electric power stations for more factories, followed by more railroads and more public schools for primary, secondary, trade, and university education. All these things combined promised better goods and services, with everyone sharing some slice of the burden. Similarly, as the theory went, more computing power concentrated inside data centers meant lower customer costs.

According to the Government Accountability Office (GAO), cost-cutting is vital because the federal government's bill for information technology overhead is $67 billion a year.[9] As part of the 2019 Federal Cloud Computing Strategy, the DOD has made some reductions by shrinking its brick-and-mortar presence and consolidating cloud management into fewer, higher functioning facilities.[10] While the GAO says the consolidation's results are unclear, it could translate into cost savings for taxpayers. The savings mean more cash for artificial intelligence (AI) research and development, small-business grants, or newer Next Generation Air Dominance fighters on the tarmac.

The Intelligence Community began its move to the cloud in 2013. Then Director of National Intelligence James Clapper led the effort to virtualize all 16 agencies' standalone computers into one network called the Intelligence Community Information Technology Effort (IC ITE), better known as "Eyesight." At an Association of Old Crows meeting in Washington that year, Clapper touted the windfall: "If we're going to make big savings in the Intelligence Community it will have to be in our IT enterprise."[11] That savings came from cost reductions in heating, ventilation, and cooling for the older machines, as well as similar reductions in electricity and maintenance bills.

At the time, the Intelligence Community was still reeling from former Central Intelligence Agency contractor Edward Snowden's revelations and how much damage one insider can do to national security. Snowden held sole superuser rights to many National Security Agency databases, too, a fact that slipped past Fort Meade, Maryland's security. If there was a way to track people's access to classified information by keystroke logs or metadata identity tagging, Clapper was for it. "The bumper-sticker mantra for IC ITE is 'tag the data, tag the people'. . . . So that if we tag the data, then we have the assurance as to the bona fides of the handlers, and can audit that, [it] would go a long way to promoting security."[12]

"Goldfinger"

A cloud's potential benefit—to be a formidable pool of data and machinery—also happens to be its primary potential vulnerability. Since Snowden, the re-

sponse of the Defense Department and the Intelligence Community has been to recentralize and pack the cloud into select "Fort Knox" data centers. Then the defenders erect virtual ramparts with redundant firewalls, routers, and proxy servers or put public cloud providers on contract to do it for them. "Fort Knox," said Harvard professor Jonathan Zittrain in 2010, "represents the ideal of security through centralization—gunships, tanks, and 30,000 soldiers surround a vault containing over $700 billion in American government gold."[13]

And that gold—the command-and-control data for the on-ramps—is very precious, indeed. Moving it rapidly to the people that need it is key to the success of ABMS. To hoard it all away from malign actors under one roof (or within one system of systems) seems logical.

But commingling data from every service could pose some thorny policy and security problems. Cybercriminals are lurking. The antivirus company McAfee estimates the global cost of cybercrime is about $600 billion annually.[14] A 2020 Price Waterhouse Coopers survey ranks cybercrime as the government and public sectors' most disruptive event with an estimated $42 billion in losses in the last two years alone.[15] Like the eponymous 1964 James Bond movie *Goldfinger*, seizing a target with an impregnable appearance could be an irresistible prize to criminals that carries very real—and potentially devastating—consequences.[16]

This scenario certainly paints a tantalizing picture, though an unforced human error could be just as damaging. Along the outskirts of Northern Virginia is Amazon's most extensive data hub for Simple Storage Service (S3). On February 27, 2017, administrators detected a bug inside S3's billing system. Once the problem was isolated to a specific subnet, they hastily followed a standard procedure to resolve it. But A miskeyed script removed a large group of the massive network's index servers. The East Coast operations of AWS momentarily froze. S3 could neither accept new virtual machines, retrieve location information, nor process requests until the problem was corrected five hours later.[17]

Nature's fury plays a part, too. Ten regional hubs host Azure's software development tools. They must be kept cool to operate at peak efficiency. But when a severe lightning storm lashed South Central Texas on September 4, 2018, power spikes jolted a nearby Microsoft data center's air conditioning. As temperatures inside rose, an automated, step-by-step shutdown process went into effect to reduce equipment damage and prevent data loss. After 21 hours, normal service was restored, followed by a public inquiry citing "cross-dependencies" that caused a cascading series of outages worldwide.[18]

"Don't Be Evil"

A public cloud's democratic appeal has also contributed to a phenomenon known in the industry as multitenancy. Private DOD clouds are reserved for DOD members who undergo a strict security background check before starting their work. They have some assurance of the soldiers or sailors neighboring them and work (mostly) without any political or social factors to disturb them. But experts say external tenants—outside the Department and the federal government—warrant a watchful eye. Private citizens, foreign countries, and other rogue entities inhabit the for-profit public cloud, too.[19] In one notable example, AWS suspended Parler's account following the January 6, 2021 insurrection on Capitol Hill.[20] The social media outlet is a favored alternative for alternative-right users who violate Facebook and Twitter's codes of conduct regarding hate speech.

More complications between the tech industry and the military have arisen. Though Google's AI engineers are responsible for creating some of the most advanced software for image recognition on the market today, the Silicon Valley giant began to have ethical doubts about its contract with the DOD's Project Maven in 2018. Maven's algorithms sift through thousands of hours of reconnaissance drone footage, pinpointing buildings, people, and vehicles that human analysts tag. In an open letter to Chief Executive Officer Sundar Pichai, thousands of Googlers said the relationship violated their "Don't be evil" motto.[21] Pichai found their argument had merit and approved the agreement's termination. It bowed out of consideration for the Joint Defense Enterprise Infrastructure, saying the contract's sole sourcing also violated its corporate principles. The head of Google's Open Research group, Meredith Whittaker, praised the end of the controversial alliance over Twitter: "I am incredibly happy about this decision, and have a deep respect for the people who worked and risked to make it happen. Google should not be in the business of war."[22]

Former Deputy Secretary of Defense Robert O. Work is an early founder of Project Maven who chaired a recent government commission on AI's strategic importance. He reacted, saying Pichai's call was "motivated by an assumption that any use of artificial intelligence in support for the Pentagon is a bad thing. But what about using artificial intelligence to power robots that defuse bombs or improvised explosive devices? Or using AI to prevent cyberattacks on our electrical grid?" The parting of ways marked the end of a dark chapter in Silicon Valley's history of innovative partnerships with Washington and the military. "Not being able to tap into the immense talent at Google to help DOD employ AI in ethical and moral ways is very sad for our society and country," he added. "It will make it

more difficult to compete with countries that have no moral or ethical governors on AI in the national security space."[23]

The Hybrid Option

Private and public clouds aside, a third option is a hybrid cloud. Hybrid clouds combine a private cloud's security and customization with a public cloud's high-speed computer processing. They are ideal for organizations that do not want to deal with a commercial cloud's baggage and the unanticipated cost. Google and Amazon have been industry leaders in selling customers on a preset menu of tools to use on their public platforms. Microsoft and IBM have been more flexible by comparison, allowing users to deploy their cloud tools on their existing on-premises networks. Due to the computer code's iterative nature, all companies charge per second, use, and gigabyte.[24] One struggling IC program that could not be named due to its work's sensitivity accrued $1.5 million in AWS charges in one year. Researchers with finite budgets and periods of performance try to find their way around these challenges, and it is not easy.

One solution is a private, hybrid cloud owned by the government and operated by cleared defense contractors. It could provide a haven for ABMS ideas to "fail-fast" Silicon Valley-style or win quickly. This way, a project's financiers can see what works, renegotiate contracts, and move on, if necessary. Also, both major public competitors—AWS and Azure—can process secret-level information. Disturbingly, only Amazon is accredited to process top-secret data, and Microsoft is likely to follow suit.[25] A previous edition of *Air & Space Power Journal*, however, made a case for Technology for Innovation and Testing on Accredited Networks (TITAN).[26] That system is a good example of a private, hybrid cloud overseen by Headquarters Air Force that can process all the same information for a flat fee. Such an arrangement could likely help the government avoid an uncomfortable vendor lock-in situation in the future.

Without question, like any monumental task, shooting down cruise missiles with data has its risks. Choosing the right kind of cloud should not be one of them. The Air Force's partnership with private industry has helped counter US adversaries abroad for generations. Keeping that partnership healthy and alive will be critical to growing cutting-edge ABMS ideas inside a hybrid cloud that is safe, affordable, and secure.

Maj William Giannetti, USAFR
Major Giannetti (MS, St. Joseph's University) is the 62nd Airlift Wing's reserve senior intelligence officer and TITAN's former director of operations.

Notes

1. David Axe, "One Battle System to Rule Them All," *Combat Aircraft Journal* (December 2020): 96.
2. Theresa Hitchens, "ABMS Demo Proves AI Chops for C2," Breaking Defense, September 3, 2020, https://breakingdefense.com/.
3. Theresa Hitchens, "Roper Pushes Moving Project Maven to Air Force," Breaking Defense, June 11, 2020, https://breakingdefense.com/.
4. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US Department of National Institute of Standards and Technology (NIST), special publication 800-145 (Gaithersburg, MD: NIST, September 2011), https://csrc.nist.gov/.
5. Robert Coram, Boyd: *The Fighter Pilot Who Changed the Art of War* (Boston: Little, Brown, 2002).
6. Antonio Regalado, "Who Coined 'Cloud Computing'?" *MIT Technology Review*, October 31, 2011, https://www.technologyreview.com/.
7. Tim Maurer and Garrett Hinck, *Cloud Security: A Primer for Policymakers* (Washington DC: Carnegie Endowment for Peace, 2020), https://carnegieendowment.org/.
8. "Economies of Scale and Scope," *Economist*, October 20, 2008, https://www.economist.com/.
9. US Government Accountability Office (GAO), *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Need to Be Better Tracked* (Washington, DC: GAO, April 2019), https://www.gao.gov.
10. Office of the Federal Chief Information Officer (CIO), *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, DC: CIO, 2019), https://cloud.cio.gov/.
11. Jordana Mishory, "DNI Clapper Pegs IT Enterprise Effort as Best Way to Save Money," *Inside the Pentagon* 29, no. 44 (October 31, 2013), https://www.jstor.org/.
12. Mishory, "Clapper Pegs IT."
13. Jonathan Zittrain, "The Internet's Fort Knox Problem," Future of the Internet and How to Stop It (blog) June 3, 2010, https://blogs.harvard.edu/.
14. McAfee, *The Economic Impact of Cybercrime: No Slowing Down* (Santa Clara, CA: McAfee, December 2017), https://www.mcafee.com/.
15. Kristin Rivera et al., "2020: Fighting Fraud: A Never-Ending Battle: PwC's Global Economic Crime and Fraud Survey," Price-Waterhouse-Coopers, 2020, https://www.pwc.com/.
16. Maurer and Hinck, *Cloud Security*.
17. Amazon Web Services, "Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region," https://aws.amazon.com/.
18. Buck Hodges, "Postmortem: VSTS 4 September 2018," Microsoft Azure DevOps Service (blog) September 10, 2018, https://devblogs.microsoft.com/.
19. Maj Steven C. Dudash, *The Department of Defense and the Power of Cloud Computing* (Maxwell AFB, AL: Air University Press, 2016).
20. John Paczkowski and Ryan Mac, "Amazon Will Suspend Hosting for Pro-Trump Social Network Parler," BuzzFeed, January 9, 2021, https://www.buzzfeednews.com/.
21. Drew Harwell, "Google to Drop Pentagon AI Contract after Employee Objections to the 'Business of War,'" *Washington Post*, June 1, 2018, https://www.washingtonpost.com/; and Lucy Suchman et al, "Open Letter in Support of Google Employees and Tech Workers," International Committee for Robot Arms Control (blog) June 2018, https://www.icrac.net/.

22. Meredith Whittaker, "I am incredibly happy. . ." Twitter, 1 June 2018, 3:28 p.m., June 1, 2018, https://twitter.com/.

23. Harwell, "Google to Drop Pentagon."

24. Maj Noah Hassler et al., "Bullet Background Paper on Commercial Cloud Usage in the Intelligence, Surveillance and Reconnaissance Enterprise," ISR-300 background paper, November 2019, 1.

25. Aaron Gregg, "With a $10 Billion Cloud-Computing Deal Snarled in Court, the Pentagon May Move Forward without It," *Washington Post*, February 10, 2021, https://www.washingtonpost.com/.

26. Maj William Giannetti, "Quiet Giant: The TITAN Cloud and the Future of DOD Artificial Intelligence," *Air & Space Power Journal* 34, no. 1 (Spring 2020): 54-58, https://www.airuniversity.af.edu/.