Event Summary: Requirements for a Successful Military Cloud: Best Practice, Innovation and Security

Participants:
- William Schneider, Senior Fellow, Hudson Institute
- Tod Lindberg, moderator, Senior Fellow, Hudson Institute
- Seth Cropsey, Senior Fellow and Director, Center for American Seapower, Hudson Institute

On July 30, 2018, Hudson Institute convened a panel discussion on "Requirements for a Successful Military Cloud: Best Practices, Innovation and Security."

This event summary addresses the major issues discussed by participants during the conference and draws on the full transcript of the event, available here: [https://www.hudson.org/research/14486-full-transcript-requirements-for-a-successful-military-cloud-best-practices-innovation-and-security]

*Hudson Institute is grateful for the support of Oracle Corporation and Microsoft Corporation in sponsoring the event and associated publications.*

Hudson Institute
1201 Pennsylvania Ave, N.W., Suite 400
Washington, DC 20004
July 30th, 2018
It has been an exciting time for innovation in the Department of Defense (DoD). About two months ago, the department, at the urging of Deputy Secretary Patrick Shanahan, initiated a draft request for proposal (RFP) for the DoD procurement of cloud-based information technology services under its Joint Enterprise Defense Infrastructure initiative, or JEDI.

After receiving industry comments and congressional comments, DoD stood down for about two months to review the subject. Then on July 26, it published a final version of its RFP. Bidders, in what is described as a free and open competition, have until mid-September to submit proposals for a fixed price to deliver cloud services for a period of two years, with extensions and renewals up to a period of 10 years. DoD currently estimates the total cost of cloud services over the 10-year period as approximately $10 billion.

DoD has been discussing this for a decade, but has been relatively slow to move. So the RFP has been greeted with a great deal of interest and controversy—in particular the RFP’s embrace of a single provider of cloud services for JEDI, at least for the first two years of the program.

**DoD Procurement: Background**


The total number of people in DoD contracting and procurement rivals the size of the United States Marine Corps. That's 150,000 in purchasing versus 186,000 Marines.

These bureaucratic cadres have multiplied as the DoD bureaucracy has expanded—with mixed results for defense capabilities. During the Reagan administration, for example, with the help of one of the shipyards in the southern United States, Congress decided to tell the Navy to spend $100 million and appropriated money to build a replacement for a Vietnam-era small boat. The procurement system, even in the 1980s, was complex, and accountability was questionable. The Navy ended up with was a 331-ton vessel that was unusable for its intended purpose.

With a procurement as large as JEDI, the number and complexity of the constituencies to be served is vast. And the process of integration will be both complex and expensive.

**DoD and Information Technology**

The Department of Defense has long had a troubled relationship with information technology. The two seminal inventions that emerged from World War II were the military applications of atomic energy and computing. At the outset, both were dominated by the government. But since the 1970s, DoD has become (relatively speaking) a minor user of computing, not a driving user of it, and this is even more so today. Accordingly, DoD has increasingly been obliged to adapt commercial technologies to its needs. And to an increasing degree, the technologies that are
shaping the commercial applications of IT are moving along much more rapidly than the DoD capacity to absorb them.

DoD processes were made for an industrial age, not for an age when information is the dominant mode in which the Defense Department operates.

**An Important Step Forward**

The importance of DoD actually making a decision to begin to move operations to a cloud-based information technology architecture cannot be overstated. The DoD leadership, especially Deputy Secretary Shanahan, deserve credit for moving forward.

The nature of military operations will no longer permit the use of modern military systems without cloud-based sources of data, not only for storage and retrieval, but perhaps more importantly, for processing—which is to say, for war-fighting in real time. These data come from many different sources—space-based platforms, airborne platforms, naval vessels (both surface and submarines), as well as terrestrial systems. These need to be integrated. And the data needs to be processed, and insights extracted from them and distributed to combatants.

Similarly, data needs to be collected, stored and processed to run the DoD logistics system and many other operations. Moving the data to a cloud-based architecture is necessary for military operations. The F-22 and the F-35 aircraft are two of the poster children for the importance of moving to a cloud-based architecture, but they are by no means the only ones.

In the move to the JEDI cloud, however, three major points need to be addressed. The first deals with the issue of best practices. One of the points that comes through clearly in the RFP is that DoD wants, to the greatest degree possible, to build on the commercial market for cloud-based services. This market has grown remarkably in the past decade. And, as a commercial product, it is quite mature. In the private sector, more than half of the enterprise-wide users of cloud services have at least five different cloud providers for different applications.

One of the defining characteristics of the DoD solicitation, however, is that it seeks a single cloud service provider. And this differs from a commercial model developed to take advantage of a vibrant industry that is capturing new technology and developing very rapidly to offer a service mix that goes well beyond merely storing data to include retrieval and processing as well. And the market has demonstrated its ability to evolve to offer these services.

A second cloud issue is security. When Director Clapper, as director of National Intelligence, made a decision in 2013 to move all of the operations of the 17 agencies of the Intelligence Community to a cloud-based architecture, one of the driving concerns was security.

The security problems that emerged under the formerly decentralized information technology architecture were producing significant losses in data. The failure to patch a computer or a mistake in using a thumb drive to take data off a specific machine was producing problems that moving to a cloud-based architecture could eliminate.
The cloud is not a security cure-all, however. DoD is going to have to provide confidence that the move to the cloud will be associated with better security than has been engineered with the existing decentralized system.

One remaining problem is the insider threat: someone whose access credentials are legitimate but whose purpose is nefarious. Another is the physical security of cloud installations. The request for proposal calls for a minimum of three such structures. Their location could be on a military base, or at some suitably concealed location. But nevertheless, a relatively small infrastructure like that is vulnerable to physical attack, and a physical attack is quite likely, given the very inviting target that such a high degree of centralization of core operational data presents.

Whether the sites number three or 30, it’s still a small number compared to the decentralized model. This will produce an inviting problem for an adversary, and a vexing problem for us. Another security issue arises with the supply chain. Cloud infrastructure—both hardware and software—need to be continually refreshed to respond to user needs, mission requirements, and the evolution of technology. The problem of preventing supply chain contamination is a very difficult one. And indeed, some units within DoD have acknowledged that it's not possible to protect the supply chain, or at least that it's not possible to have confidence that the supply chain has not been contaminated.

A third major cloud issue is preserving access to innovation. The underlying technologies that shape the ability to provide greater functionality in cloud services are changing much more rapidly than DoD processes can readily take in. Reliance on the commercial sector for cloud services makes sense from the point of view of capturing that innovation, but the acquisition process also needs to have the capacity to render it attractive for the commercial sector to continue to offer innovative services. Some of the industry comments on the draft RFP observed that it's unlikely cloud services vendors would turn a profit until somewhere between the sixth and 10th year of the proposed contract. Such rigidities in the contracting process would not offer much of incentive to the cloud service provider to provide additional services and functionality in the absence of some better way of the government procuring such services.

The “joint” aspect of the JEDI request for proposal reflects the fact that we don't fight as an Army, Navy or Air Force. We fight jointly, and all of the capacity of the military departments to operate jointly in the fight needs to be enabled. The cloud-based IT model perhaps presents the most appealing way to enable this. We can accordingly be optimistic about DoD’s initial steps on JEDI—even though DoD’s move to the cloud is likely to evolve in the way the commercial model has evolved: from an initial single-provider as the enterprise became comfortable with the notion of cloud-based applications, and then later to a multi-cloud environment.

A “Pathfinder” JEDI Contract

DoD has chosen to designate the JEDI proposal it solicits as a “pathfinder” contract. Although the term has no fixed statutory meaning in the DoD procurement process, an optimistic view of this designation would be that DoD understands the risk of being permanently committed to one approach to cloud services—in other words, that by locking themselves into a single-cloud approach, they will deny themselves access to potentially better approaches as the path forward becomes clearer.
For example, in the late 1970s, DoD adopted the Ada programming language in what it thought would be a universal language in writing code for defense products. Even such modern weapons systems as the B-2 bomber had its code in Ada. But Ada was not destined for universality, as DoD quickly learned. In fact, DoD has made a lot of bad bets in its effort to adapt information technology for its own purposes.

By now, dependence on commercial service providers, combined with a willingness not to try to tell them exactly how to do their jobs, is the default setting of DoD. That is a basis for optimism that the path DoD is taking on JEDI will allow commercial practices to dominate and set standards.

The tougher problem that DoD will face is to adapt to commercial standards. Currently comfortable with a system that is sclerotic and does not really depend on the kind of data use that would really make its systems work most effectively, how will DoD manage in a new environment? DoD will benefit most from an engaged private sector that is willing to help shape the governance model and the contracting model and the functionality that can be built into the system.

It's very hard to get big, successful organizations to change. The adaptation that the Defense Department is going to have to go through with its move to the cloud is small beer compared to what is coming: the almost complete inversion of DoD's existing model of “product development.” Instead of depending on defense technology to produce defense products, DoD will be dependent on civil technology to produce defense products. That will require a very demanding change in mindset. The case for optimism is that it's going to be the people wearing uniforms driving these changes, not the massive bureaucracy for contracting and procurement.