Hudson Institute

Making Military Cloud a Success: Critical Next Steps for DoD's IT Strategy

- Dr. Fred Schneider, *Professor, Cornell University; and founding Chairman, National Academies Forum on Cyber Resilience*
- Dr. William Schneider, Jr., *Senior Fellow, Hudson Institute*
- Dr. Arthur Herman, *Senior Fellow and Director, Quantum Alliance Initiative, Hudson Institute*

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
April 4, 2019

TRANSCRIPT

Please note: This transcript is based off a recording and mistranslations may appear in text. A video of the event is available: https://www.hudson.org/events/1673-making-military-cloud-a-success-critical-next-steps-for-do-d-s-it-strategy42019

WILLIAM SCHNEIDER JR: Well, I think we're good to go. If you missed lunch, the last train leaving the station is still out there, so feel free to go get it. But in the interim, I'd like to start off as - I'm going to try and both moderate and participate, if that's allowable in this context in our discussion of - our continuing discussion of federal IT. There's our colleague Arthur Herman from the Hudson Institute and also Fred Schneider - and I know he will say mercifully unrelated to the moderator - from - professor of computer science at Cornell University and has been an active participant in various study groups in DOD and National Academy of Sciences and so forth, so is very knowledgeable about the subjects we're going to be discussing. And we've had quite of an interesting sequence of events that shows how important and enduring this issue of federal IT is likely to be, as the concerns about the need to have us move to some sort of cloud-based architecture is spreading throughout the government. We'll have more to say about it. But in the past couple of weeks, the intelligence community has published its intent to create a substantial initiative relating to evolving how it uses the cloud-based architecture for its mission. I was involved in - as was Professor Schneider - in some of the early discussions in the DOD through the Defense Science Board on the need for the DOD to move to the cloud and, more particularly, the manner in which the data in the cloud was secured. And the IC, intelligence community, was a pioneer in doing this. They've had quite a successful run with the use of the cloud that's impressed other parts of the government. But now they're evolving their model from a cloud monoculture to a hybrid cloud environment, and they have a very interesting process about how they're going about it, which seems to closely parallel commercial practice, which is - has been an aspiration for some time. And we'll - we can have more discussion of that. So let's start with Fred and have a few opening observations and then Arthur, and then we'll have a little discussion among the panel and then open it up for questions.

FRED SCHNEIDER: All right. Thank you. So perhaps because I sit in an ivory tower, I am more compelled by principled arguments. The second law of thermodynamics, which is the reason all engines work, is that entropy has to increase unless you're prepared to expend energy. Entropy is disorder in systems. And it's served physics quite well. There seems to be an analogous law for software and systems; in particular, uniformity will erode unless you're prepared to expend energy or resources. So unless it's a closed system, there will be a tendency to have a diversity of platforms or a diversity of applications. And it shouldn't be surprising; people tend to take the shortest path, so they would use the application that is most available, or they would build an application for the environment that's easiest, best suited for that application or where there's the biggest market. And I think this is going to be a reality for the future. And if you look back, it has always been a reality for our past. Legislating for Windows platforms didn't work out all that well. Legislating for IBM systems didn't work out. And by didn't work out, I don't mean it was a bad system; I mean eventually, there was heterogeneity, and we had to accommodate it. So that would suggest that hybrid clouds are the natural order of things because there is and will be a diversity of services. And even if DOD had sufficient control to create a uniform cloud, I submit that DOD, to be effective, especially if they become very cloud-centric or computing-centric, is going to want to interact with international partners above - over whom DOD doesn't have authority and an industry base that DOD doesn't have an authority. So there is going to be a natural heterogeneity. And that says that, although letting a single-cloud contract might be an interesting first step, it would be unwise to think that we wouldn't evolve to some kind of a hybrid cloud, at any level, with regard to any function. And since there is a cost of communication between applications or services on a cloud, and you have to pay that cost. The up-charge when these things are in different physical platforms is very small compared to the up-charge of

the communication, and that says that we're not going to sacrifice anything by assuming at the outset that things are hybrid.

ARTHUR HERMAN: Good afternoon. Glad you're here. Glad to be here with my distinguished co-panelists. My approach to this issue is somewhat different from those of my co-panelists. I've not been very much involved in the development of the kinds of technologies that we identify with the cloud. My interest in this particular issue and DOD's effort to develop a single-cloud solution to its future IT comes from a diversity of perspectives. One is, as a longtime fascinated student and sometimes morbidly fascinated student of the Pentagon procurement process, I wrote a book called "Freedom's Forge," which was about the making of the arsenal of democracy in World War II. And since then, I've always been sort of fascinated by the way in which DOD goes about trying to acquire especially new, emerging and advanced technologies, and this is certainly the case here. The second perspective is that of a student over the last decade of cybersecurity issues, particularly from the point of view of cybersecurity strategy and cyber deterrence, theories of cyber deterrence, particularly with regard to advanced persistent threats, such as Russia and China. And then the third is looking - in the case of Pentagon procurement, my perspective emerges out of the past record; my current - a lot of my current work is focused on the future record, which is how quantum technology and quantum information science is going to have an impact on cybersecurity issues on the one hand but then also on the way in which the federal government and other governments and agencies will come to grips with the threat or opportunities that quantum security - quantum technology offers. And I have to say that from the point of view of - a sort of an opening view of what has happened here and what's going on, that going over the cloud strategy that DOD released that was to form the basis of the way in which they went for the single-cloud solution. And it was interesting that they found a vendor first and then developed a strategy afterwards as a way to go about it. One would think it's putting kind of the cart before the horse. But that's - these are archaic metaphors; we don't use those anymore in the digital age and the post-digital age. What struck me about it was - is that the DOD - that what I saw in this strategy, in this effort, was a valiant attempt to integrate an advanced technology in order to modernize the information technology infrastructure for DOD as a whole, an attempt to integrate and to reach out and to adopt that technology without really fully understanding all of the challenges or all of the risks, as well as many opportunities that that technology involved, with the hope that by choosing a single operator, a very competent and very experienced operator, that it would be up to the operator to solve all of those problems that DOD didn't want to address and didn't want to come to grips with. So - and I think that's kind of where they find themselves now, is that, in fact, there were a lot of (laughter) problems and issues that they should have thought about before going out and choosing the vendor, before starting this process, but that now maybe they need to go back and rethink some of those and maybe come up with a different model and a different - and look to other best practices as a way in which to go about that. So from where I am, I would say, for DOD, A for effort, but a much lower score for results and method for going about it.

WILLIAM SCHNEIDER JR: Well, I think one of the issues that we need to consider is the problems that the Defense Department has, generally, with adapting new technology that is primarily located in the civil sector. There's been a number of tries in how to do this. The Defense Innovation Unit Experimental that Secretary Carter set up a couple of years ago was reflective of an attempt. But one of the interesting things about IT that really makes it hard to square with the DOD culture is that the custom in software, for example, has been to sell products to the consumer that the producer knows are defective - that the relationship with the -

between the producer and the consumer is such that the consumer will find the problems, the producer will make the fixes and evolve the software in ways that really becomes useful to the users. And by being able to do this at scale, they are able to have a very short development cycle compared to the customs in the Department of Defense, where there is a very high bar to reliability, very high bar to technical maturity and so forth. All of these things differ significantly from the I.T. sector, and I think the experience that the national security community in general has encountered with acquiring cloud services reflects that kind of difficulty. But I think the way the intelligence community has proceeded has some interesting features that are worth studying - that they have gone from a monoculture to a recognition that a hybrid architecture is necessary. I think DOD has a similar view in the sense that there are already 500 cloud service providers providing such services to the DOD; what's missing is the integration of it, which is the aspiration that the DOD has not yet been able to resolve. But also, the movement to a large number of cloud service providers has other security issues relating to the attack surfaces, and Fred, maybe you might have some things to add on that point.

FRED SCHNEIDER: Right. So attack surface is a metaphor for the surface area that's available to the attacker. Think of a wall - a longer wall has a lot more places you might try to penetrate. And people talk about the attack surface for a system. If we were to build a hybrid cloud, then there would be lots more features, lots of duplication of function in different pieces of software because each of the cloud providers would have had to build the same functionality. It only takes one vulnerability to get in, and so one argument against having a hybrid or a heterogeneous cloud is that it has an increased attack surface. A monoculture would seem not to have this problem, but it has a different problem, which is that it's much simpler so that your attacker has an easier time analyzing it. Your attacker also has an easier time focusing attention on it. So if you wanted to do a supply chain attack, it would be easier because there are clear destinations for the things you have to compromise. So there's this funny sort of tradeoff, and to my knowledge, nobody has been able to make a good analysis of how the tradeoff works. If you use metaphors, you can think of a hybrid cloud as either giving you - it could either be as weak as the weakest link; it most certainly will unless you design it so there is an internal resilience - that is, if one piece is compromised, it's hard to leapfrog into other pieces. Or you have the opportunity to inherit the best practices from any one of the components into other components. Both of those are really management issues; they talk about how the clouds are composed. And it's a set of interesting design choices that you have to make, but you have to make them also in a monoculture because there will be diverse components, different applications and so on. You want to make sure that if one of them gets compromised, it's not possible to leapfrog into another. So it would seem that the costs of being hybrid over mono are not significant, but the same sets of problems exist, and you need to confront them. I assume once DOD gets to the point of letting a contract, they will start worrying about how to deal with that.

WILLIAM SCHNEIDER JR: Just a dimension of this that's changed in the last year or less has been the aspiration of DOD, in response to concerns about the security of the supply chain, is this requirement to deliver - for the vendors to deliver products that are uncompromised. There's a good study that was done by MITRE. It's an unclassified study that describes this - "Deliver Uncompromised" - but it adds a new level of burden to vendors. And we've seen the consequences already of a very limited imposition of cybersecurity discipline, where the prime contractors are now required to cascade to their subcontractors an affirmation by the subcontractor that they have complied with the the cybersecurity regulations that the DOD has - have promulgated. Well, that single contractual provision cost 20 percent of the DOD industrial

base to drop out of the market. It's because they are smaller companies, a small part of their business is involved with DOD, and they are generally not enthusiastic about the combination of a small business base, large liability and high cost to execute. So I think it illustrates this tension that Fred was referring to, about how the DOD is going to be able to manage its IT, as it's tied into the defense industrial base and the way it procures products. It's an increasingly complex matter, and I think if you look at the - this concept of deliver uncompromised, I think it's going to be a pretty significant one. We've - you've probably heard about the likely reorganization of the Defense Security Service, where it's going to get an expanded mandate to do government-wide personnel vetting, not just DOD, and they will have some responsibilities for some form of surveillance over the the supply chain because of this deliver uncompromised aspiration. So you have the underlying IT infrastructure that is, you know, going to be cloud-based, probably hybrid cloud-based, but interacting with the entire organism, going from the pointy-end of the spear with the operating forces to the small mom-and-pop shops that are delivering defense products and services to the department. So it's a much more complex ecosystem that's really going to be integrated by this cloud-based architecture.

HERMAN: So what you're really saying, Bill, is that there's going to be a number of small contractors. And I've worked with some of those small contractors in terms of the kinds of challenges they face, in terms of economies of scale - not just competing with defense contractors but also within the DOD acquisition process. They're going to find themselves increasingly frozen out by the kind of requirements that this new IT infrastructure will make on them.

WILLIAM SCHNEIDER JR: Yeah, well...

HERMAN: Especially if, as is according to the cloud strategy document anyway, a lot of that requirement will be that data to be encrypted. And this is part of the way in which they see them providing the kind of defense against cybersecurity attack - will be that, as they put it in the report, not so much defending the perimeters, but rather instead protecting the data by having it encrypted within the cloud structure as well. And that's going to be yet another layer of requirement that's going to be put on companies that may sort of say, I just don't really know if it's...

WILLIAM SCHNEIDER JR: Yeah, well, that's - you know, poses a risk to the industrial base, and it wasn't quite captured in the recent White House document that covered some of the more, I would say, industrial aspects of the defense industrial base rather than some of the kind of things that we're discussing. But there's no doubt that the management problems associated with this - managing this infrastructure, when the principal threat to the industrial base is now coming from cyber operations by adversaries, it's a much more difficult problem. And as we've seen in the importance of intellectual property, modern defense procurement, for the most part, has inverted the paradigm that we've seen for most of the 20th century, where most of the cost of a defense system was in its procurement, not its development. But that's being inverted, where most of the costs are in the development, not the acquisition of the product. Many years ago, when I served in the Office of Management and Budget, we were buying about 1,500 aircraft a year; you know, now we're buying a couple of hundred aircraft per year because these systems are rendered much more capable by their interaction with the sensor network and so forth. And so the industrial aspects of it are changing, and that's going to be reflected in the IT ecosystem that supports it.

FRED SCHNEIDER: So I would say that having data being encrypted is the least of our problems. What's needed in order to make a bunch of subsystems be resilient is a lot more than making sure the data is encrypted. There are ways of establishing trust, and the best way to simplify that is - what about the keys? They have to be taken care of, and if they can be compromised, we're in trouble. So the first step really needs to be some kind of understanding of what is compliance - what do we require of these software systems and hardware systems to be trustworthy enough for use by DOD? We have a really bad track record in the industry and in government of defining compliance for IT systems, dating back to the Orange Book, which was our first exercise in that. And there are two risks - one is you require people to do things that don't actually solve the real problem, and that may have the effect of causing players to remove themselves from the marketplace; the other issue is compliance could be a prescription that impedes innovation and progress. And certainly, when we're at the beginning of the lifecycle of a technology, like we are for clouds, you don't want to be impeding progress. And security in a cloud is particularly problematic, and so there is likely to be a fair bit of innovation there in the next five to 10 years. So DOD has this challenge that they need to get onto a cloud soon, and what's out there is probably not trustworthy enough for all the needs. And they also need to figure out - what is the prescription? - so that any cloud provider can contribute. And that's not the challenge of what the cloud provider has to do. that's the challenge of what - let's define the height of the bar, so to speak.

HERMAN: And you're saying DOD's not done such a great job?

FRED SCHNEIDER: DOD hasn't done a good job of this, but let's be clear, nobody has. It's a really hard problem. It's not because the DOD is incompetent; it's because it's a technically difficult challenge.

WILLIAM SCHNEIDER JR: The compliance issue is really an important one and I think is one of the things that DOD was trying to - is trying to get at with its movement into a disciplined defense-wide cloud environment, is the issue of compliance. There was an interesting vignette in one of the defense trade journals this week, where they were reporting on an exercise that was taking place between artillery units of the U.S. Marine Corps and their Australian counterpart. And some piece of information that was essential to the collaborative and integrated operation of the two countries' artillery battalions was because of some oversight. They were not - the U.S. Marines were not allowed to share the data with their Australian counterpart. They went back and got a waiver on it so they were able to to go ahead, but you can obviously see that, in a tactical situation, this would be, you know, totally destructive of the ability of allies to work together. And that's why, in a compliance sense, if we're going to interoperate with our allies, we need this ability to manage the compliance process so that we are able to interoperate. But it will have a tremendous benefit of avoiding the kind of problems that we've had in the Kosovo air campaign or the air campaign against Libya in 2011, where the allies really can't interoperate because they're not able to share data in a way that's relevant for tactical purposes, even among allies that have the closest bonds of trust and collaboration. So all of these things are starting to get poured into this stew of data sharing. I'm reminded of a phrase attributed to Eisenhower that I think may fit well into this situation is that, the way to solve a hard problem, he said, was to make it bigger - where you put the hard problem, embedding in a much larger context, in which case the difficult but small problem sometimes becomes easier to manage in that case. And I think if we start to recognize the tremendous

benefits that can accrue to an ability to share data more routinely, that it will enable us to solve some of these problems that are going to be embedded in a resolution of the compliance issue.

HERMAN: Yeah, and especially if we have - the interoperability issue is going to run up against the question of - we have an IT infrastructure which has a certain level of compliance, certain kinds of standards, but we're interoperating with allies who may depend upon systems and platforms about which we don't particularly have a lot of trust; I'm thinking in particular with regard to 5G. And as more and more of the information that's shared even by military services is on commercial networks, if those commercial networks are, let's say, being operated by companies such as Huawei, you may have problems that would begin to arise in terms of the ability of information that's contained on the cloud, of wanting to be able to share that even with trusted allies because of the interface between the two different types of platforms.

WILLIAM SCHNEIDER JR: I suspect there won't be much sensitive information that moves on commercial networks, anyway. It will probably still be done with dedicated networks, but that doesn't say with 5G that the hardware may still be Huawei in some cases.

HERMAN: Yeah, and of course, from an intelligence gathering point of view, there's a lot you can gather from unclassified data that could also be extremely challenging to deal with, too.

WILLIAM SCHNEIDER JR: Yeah.

FRED SCHNEIDER: I do believe in encryption.

HERMAN: Yeah.

FRED SCHNEIDER: You can put encrypted data even on the Chinese networks, and you're OK.

HERMAN: For now. For now.

WILLIAM SCHNEIDER JR: Yeah, providing that the key hasn't been compromised.

HERMAN: Right.

FRED SCHNEIDER: Well, if the key is compromised, all bets are off (laughter).

WILLIAM SCHNEIDER JR: Yeah.

HERMAN: Well, that raises, of course, the other issue that's gotten me interested in this whole topic, and that's the issue about the possibility of future quantum intrusion. And although some of us may disagree on exactly when that - what the timeline would be for such a quantum intrusion, it is a real enough possibility, if not necessarily probability, that we may face a near-peer competitor who would have that capacity to deal with it. So one of the other challenges that would have to be taken on for developing a DOD cloud solution - hybrid or single cloud, whichever way they decide in the end to go - will be to find ways in which to make it quantum-resistant to prevent quantum intrusion in the future. And this - I guess I can see this - and here I defer to my two co-panelists. What I also see is one of the other challenges that was not particularly well-addressed, I thought, in the cloud strategy. And a discussion coming out of the DoD about this is the issue of the timeline of the technologies involved. I mean, this is a cloud project which is to extend out over 10 years. And in the course of that decade, lots is going to change with regard to the technology, including possibly having the possibility of a quantum

computer that could disrupt or decrypt encrypted information and data networks. And understanding that threat - my apologies - understanding that threat becomes one of the issues that I think that also get - that - my feeling was DoD sort of felt, well, our operator will deal with those kinds of challenges when they come up instead of addressing them from the very beginning and thinking about how - what DoD's on strategy was going to be in the cloud.

WILLIAM SCHNEIDER JR: You know, quantum applications are probably some time off compared to the likelihood that 5G telecommunications is going to be fielded. Even Chicago and Minneapolis are getting 5G this month as, I think Verizon, rolls out its first commercial application of its own. You know, 5G is going to be part of the mix. But it does reflect the fact that the government in general and the defense establishment in particular has trouble adapting its processes to take advantage of the technologies at the pace they're being developed. We've discussed, you know, three different, you know, big changes that are affecting DoD that are still not fully integrated in their operations. Cloud-based architecture, even though they're extensively used for mission-specific applications, they're not operated in an integrated manners yet. The aspirations that deliver on compromise, recognizing the threat to the supply chain, again, is an aspiration rather than something that's being implemented. And then of course, the ability to communicate data reliably and securely over - throughout the network is still an aspiration rather than something that's going to be achieved.

FRED SCHNEIDER: So a key underlying issue, even for quantum, is agility. And if you want to stay up at night worrying about quantum, then you should worry that we need to quickly switch all our cryptosystems and other things so they're quantum-resistant. But you don't - there are better things to worry about. Last spring, a group of attackers announced a way to compromise any processor chip that is using caching for - to increase the performance of memory references. If that sounds technical, I just said every semiconductor manufacturer processor is vulnerable to this. Spectre and Meltdown are what it was called in the press. So all the cloud providers have processors that have this property, which means all the cloud providers currently are vulnerable to this kind of attack. And it looks like it's a very hard thing to change. Not - and I don't mean it's hard to change because you have to buy a zillion processors and replace it. That's one headache. We don't know how to build fast processors that don't have this vulnerability in them. So whatever we adopt, we need to adopt something that has agility capabilities so that, as these problems get discovered, we can deploy solutions to them or fixes for the time being. And that's going to be an element of a compliance definition. And yet, you don't see the cloud strategy document talking about it. Everybody has this DoD-centric view. You know - I buy the fighter, and then I fly the fighter. Well, buying a computing system is the beginning. And we need to count on changing it more or less frequently as attacks get discovered and certainly as we want to add functionality.

HERMAN: Can we go back for a minute to what Bill had talked about, which was where the intelligence community is on all this? And it might be helpful for the audience to review exactly what - you know - and we're thinking about in terms of best practices of what's happened within intelligence community and approaching the issue of cloud for IT infrastructure, where the single cloud approach was the one that I see adopted in 2013, if I'm not mistaken...

WILLIAM SCHNEIDER JR: Right.

HERMAN: ...Which DoD then used - suggested was that's the lead we need to follow because those guys over there know what they're doing with regard to information technology. And how

significant is this shift now that we're seeing for where CIA wants to be with regard to a more hybrid cloud approach?

WILLIAM SCHNEIDER JR: It's not only CIA. It's the entire...

HERMAN: Right.

WILLIAM SCHNEIDER JR: ...Intelligence community. But I think it seems to parallel the commercial practice. The intelligence community solicitation talks about a sequence of surveys that would be taken of the industry that would elicit the technical approaches that they would undertake to meet intelligence community needs. And this would be extended over a period of more than a year, which would then inform the process of running the solicitation. But the solicitation, at least as far as the documents that were distributed to the industry a week or two ago, show that the - it would enable the intelligence community to capture the pace and anticipate a change of technology but also to recognize where certain providers would be able to offer better services for specific mission applications as a dimension of how they would go to a multi-cloud environment, which seems to parallel commercial practices where at least medium- and large-sized companies use between five and a dozen different cloud service providers, reflecting the specialization of labor that responds to Fred's observations about this second law of thermodynamics...

FRED SCHNEIDER: (Laughter).

WILLIAM SCHNEIDER JR: ...Which is not something that comes to mind immediately in a discussion about IT architecture.

FRED SCHNEIDER: So I think you can ask what - how things are going to play out, and there is the predicting the future, but for all possible futures, DOD's going to let a contract - it may be the first contract of many, or maybe it's the last contract if they do what they said they were going to do. And you might ask, what's the right way to proceed? Well, we already established one thing is to come up with a notion of compliance and, presumably, educate a workforce so that they can build compliant applications and make sure there's a market so that these things exist. The - presumably, whoever gets this contract is going to be told about threat information because, if DOD understands the threat really well and doesn't tell its partner, then the chances are reduced that the partner will be able to defend against attacks. And it's going to be tempting to treat the partner as being privileged. But if you believe that the entire nation will benefit if all cloud providers are more trustworthy - because, after all, even things that the DOD doesn't do are important for our survival - and if you believe that DOD actually benefits if it's non-contractors are more trustworthy because the industrial base benefits and because there is a - now a bigger set of choices if DOD ever wants to consider adding other clouds, then it's in DOD's interest not to treat this first contractor as special and to share detailed threat information with as many cloud providers as are interested because they will use this, and they will secure their clouds in turn; in fact, they may even do it in a way that innovates, and so we've had a broader space of defensive innovation. Of course, a cloud provider is only going to respond with investments to deal with this threat information if they believe they have some incentive. And the incentive is either business from DOD - well, that's back to the idea of, maybe we should think of having the first of many contracts or incentives because the customers of - the contractors to DOD, this deliver uncompromised service, and that's back to the compliance document. So I think it's important for whatever happens for DOD not to think in terms of being parsimonious

with the threat information, that the whole ecosystem will benefit if DOD at least thinks in terms of creating a very cloud - a very healthy cloud landscape. And it will give DOD a lot of flexibility.

HERMAN: What you're suggesting - and correct me if I'm wrong - is that if done right, DOD could use this as an opportunity to raise the standard of cloud security for all operators, not just for the ones that it will be working with, that one could actually have an effect all the way through the system?

FRED SCHNEIDER: Right, that would be my hope.

HERMAN: Yeah. Think it will happen?

WILLIAM SCHNEIDER JR: It's difficult to do it in the classic way in which threat information is shared because of the risk posed to sources and methods, and the way in which information on cyber vulnerabilities is collected would jeopardize the sources and methods. However, there may be other ways in which the threat data can be shared that would - instead of compromising the origin or how the data was collected, it would be more in the direction of prescriptive recommendations as to how to behave because a certain threat is out there, and rather than sharing what we know about it...

HERMAN: Information about the threat.

WILLIAM SCHNEIDER JR: Right.

FRED SCHNEIDER: Well, sharing information about vulnerabilities doesn't reveal sources and methods. And it does lead to a more...

WILLIAM SCHNEIDER JR: Right. The way in which they - the few companies that have had access to cyber vulnerabilities has involved them in access authorizations that jeopardize sources and methods. But I think it's an issue that can be managed. And it would just require a slightly different approach to the way in which threat information has been handled. But I think it can be managed. Perhaps it might be a good time to start some questions and answers 'cause we probably raised more questions than answers. Ma'am? Could you identify yourself and...

HERMAN: And wait for the mic, too.

WILLIAM SCHNEIDER JR: Yeah.

AUDIENCE MEMBER: Recently, the Defense Innovation advisory board, which is chaired by Eric Schmidt, issued a report on software acquisition - on the software acquisition process, which made a voluminous set of recommendations about adapting the current defense procurement process to enhance agility and things of that nature. So I was wondering if you all saw that as being an effort that might contribute towards more effectively implementing the cloud strategy.

WILLIAM SCHNEIDER JR: I went through the document when it was published, and there are a lot of good ideas. Having participated extensively in the government advisory process, it also has some properties that are a little different than - if you're a corporation and you get advice from McKinsey, you know, the board is breathing down your neck to either accept or reject the advice from a consulting firm or advisory body. In defense - or in government in general, the lifecycle of advice is much more protracted. Similarly, the Navy published - have an unclassified document about their own cyber-vulnerabilities. I think these documents are taken seriously, but

the implementation is balkanized over a large number of institutions within the defense establishment. So I think that this is an occasion where this compliance mechanism that we've discussed for the support of a cloud-based architecture might be a way of leapfrogging what is otherwise a very slow process that sort of mimics the DoD acquisition process and might get some of these fixes into the system more rapidly.

HERMAN: I did an article for Wall Street Journal about five years ago - maybe more - on - that - which posited the thesis that the way in which to start reforming the Pentagon procurement process as a whole was in software acquisition and procurement and that there was the perfect example in which you could try and get the Pentagon mentality to shift towards a way in which there was a - this was a constantly evolving - this is the point Bill was raising earlier - nothing comes out perfectly off of - in terms of software; you have the alpha and beta phases that go with it - and that this would be a way in which not only to facilitate the most important and growing area in terms of defense technology and innovation but also a ways in which you could compel the procurement process to move out of the old Hadley tank approach to these kinds of things to adjust to modern high tech. And what I am thinking more and more, however - and I think that this cloud issue, in my mind, fits into precisely the kind of Eisenhower solution that you want. And that is to take this problem and fit it into a bigger problem, which is - how do you get Pentagon and national security agencies as a whole to adapt more quickly to the characteristics of advanced technologies? And that's one of the projects that I'm getting underway here at Hudson to work on. And the software procurement issues and the reasons why it is aspirational as opposed to a goal, I think, goes to what we need to do in order to bring about the meeting between the need for reforms and being able to implement reforms that address the problem underlying.

WILLIAM SCHNEIDER JR: So far, it's unblemished by success, however, because the problem - reason why it doesn't work is because of the interaction of software upgrades, which are possible on an incremental basis more or less continuously. It doesn't work with the operational test and evaluation community, which needs to test the performance of the system. And if you have a small change in the software and then have to have a $200 million series of flight tests to make sure that doesn't do any harm, it doesn't work, which is why you have these several-year gaps between block fixes in say, F-35, where they...

HERMAN: That's a classic example.

WILLIAM SCHNEIDER JR: ...Put them all together. So - and the DoD is probably going to have to face reality on this issue when they go to autonomous systems because the autonomous systems can react in an infinite number of ways. By definition, you can't test an object in an infinite number of ways to ensure that it meets the requirements, so there's going to have to be some adaptation to the reality of software. But I agree, it's a good place to start if we can. I think he was next.

AUDIENCE MEMBER: Is your utility function of blockchain introducing access and information in and out of a cloud? So far, that half of it has been proven to be almost hack-proof until somebody comes up with a solution. A Cornell professor, by the way, actually told the world the way you destroy bitcoins is you steal the bank or the wallet as opposed to cracking the currency. Those are two questions.

WILLIAM SCHNEIDER JR: I'm sure Fred has some something to say about it also, but there is a serious effort being made to look at the application of blockchain to the logistics system, and it

seems as if there will be some good opportunities there. But it also may be the case that nothing's unhackable, that - and you also have to consider the very real vulnerability of communications links over which the information travels when it's in motion, and there are other vulnerabilities when it's at rest. But still, I think the - certainly, the application of blockchain looks promising for the logistics system. Fred, you have a...

FRED SCHNEIDER: Yeah. I want to comment on - first on the data at rest versus data in motion. There seems to be great benefit from sharing data as a way of allowing separate systems to cooperate in solving a problem. The Navy has embarked on a new - I'm not sure what the right noun is, but they are thinking about it. Divide the battlespace up a bunch of - across a bunch of ships. You can think of a naive division which says every ship is worried about the area around the ship, and you can think of a more sophisticated solution where certain ships specialize in certain functions and cooperate with each other. One shoots, one sensor - OK. So that only works if you can deal with data in motion, and that seems to be a way to get much cheaper solutions to many of our problems. Therefore, I think we don't have the luxury of building systems that only have data at rest. As far as bitcoins and blockchains - actually, there is a Cornell professor, my colleague, who did break bitcoin, not by stealing a wallet, but by showing how you could incentivize a number of coin miners to take over the majority. But more generally, blockchains are today's implementation of an age-old technology which you can think of as a ledger, where - that you update in ink. And we have been building systems that way forever, even from the paper days. And so there is nothing radically new there. Using it as a currency is radically new, but that's something that's spun off on its own separate thread. DOD's use and most enterprise's use is to just use it as a ledger, as a way of recording facts, sequences of events. In 2000, there was this big fuss about rewriting our software to deal with the year 2000 problem; there was a concern that much software wouldn't work well after New Year's Eve. And it turned out nothing - we must have done a great job because nothing failed. And if you can imagine all the rewriting that was done, that - on the other hand, the way to look at it is all that stuff needed to be rewritten anyway, and it was a good excuse to rewrite it. And I think we can look at blockchain as the same thing. There is a lot of crufty distributed software out there, and if blockchain is the sexy name that's going to prompt companies to redo it and update it, then we'll all be better off. It'll be much cleaner software. But they're likely not taking advantage of the esoteric, novel aspects of blockchains.

HERMAN: And still quantum-vulnerable.

FRED SCHNEIDER: Well, it depends on what crypto system you use.

HERMAN: Yeah. Well, right. And right now, in fact, there is a couple of companies working on a quantum-resistant blockchain ledger. But the point is - and I think here, Fred and I will be in agreement - that people look for magic bullets from the point of view of cybersecurity. You know, if we just have this in play - if we just have blockchain or if we just have quantum-resistant algorithms, then that takes care of the problem. It's a much more complicated evolutionary process.

AUDIENCE MEMBER: I did not count (inaudible) anticipate Snowden (inaudible).

HERMAN: (Laughter) Well, there's always that, too. There's always that.

AUDIENCE MEMBER: (Inaudible).

HERMAN: Yeah. Yes, sir?

FRED SCHNEIDER: It's coming.

HERMAN: Microphone is en route.

AUDIENCE MEMBER: So the concepts of agile acquisition and the need for cloud to require a completely different IT management and a sourcing approach, I think, is becoming more apparent because when you try to apply a weapon systems model to any IT program (laughter), you get an expected outcome of failure - and 84 months later. So what I'm concerned about when looking at JEDI and the future of C2E is that we really not address the management problems in the cloud. How do you write SLAs? How do you manage SLAs? How do you do vendor management? How do you keep the prime - for instance, C2S Amazon - from gouging all the suppliers or getting them to do things that are anti-competitive? So, you know, my concern is the lock-in and the lack of management choices and technology choices and innovation options available when a single vendor controls all cloud.

WILLIAM SCHNEIDER JR: Well, I think the aspiration is less to have a single vendor for all applications, I think, is reflected in the DOD strategy document, but a way to bring all of the cloud service providers together in a way that the organism is effectively operating through a cloud-based architecture rather than 500 clouds, as is currently the case. And I think our discussion on the compliance issue illustrated how formidable the task is of trying to get that before you even get to the vendor base. The notion of trying to transfer the concept of a prime contractor from a hardware environment that basically takes a lifetime responsibility for the maintenance of the asset. The way in which the cloud will have to be attended to is almost certainly going to require some acquisition innovation because they can't do it the way we've historically done it. And the nature of the IT industry is that it's a global industry, it uses technologies from everywhere, and that the history of consolidation in the industry suggests that this is likely to be a continuing process. And so the odds that you'll have one contractor sort of in perpetuity is probably unlikely, and so some means need to be had for managing the access to the intellectual property of contractors that come in and go out of the defense market. It's a more complicated problem that I can probably describe, but you can see the complexities out there when you're trying to adapt new technology to an old acquisition system.

FRED SCHNEIDER: I wonder if there are analogies of other functions within DOD, where there is a single capability that's shared quite broadly through the service and it's managed by a small group within the Pentagon. And I can think of none. But even DTS - you can travel for the Defense Department and not use DTS. But this would be the only game in town. But one could look to other functions to learn lessons before making it as large as it...

WILLIAM SCHNEIDER JR: Well, there have been attempts when the DOD - in the '70s and '80s, when we were starting to buy the F-16, the DOD wanted to have multiple sources of engine suppliers, so they compelled the winner to donate the - his IP to the loser so that they would be able to both manufacture the same engine. I know it's hard to believe, but somehow, not all of the process information got from one contractor to the other, and so it proved to be an unsuccessful approach. But it does underlie - or underscore the difficulties with managing IP in a government atmosphere, and that's an issue that's going to have to be tackled if we're going to have an enduring private-sector-managed architecture for IT. Yes, ma'am?

AUDIENCE MEMBER: I'm a White House correspondent and a foreign journalist from Pakistan. Last week, I was at Guantanamo to cover 9/11 military commissions for 34th pre-trial hearing, which is a forever (ph) trial. And I had a talk with Commander Bajwa, who is a JTF commander, and he shared with me that Office of Military Commissions has pitched a $20 million bid for market research feasibility to connect Guantanamo to Pentagon networks. So having said that, my question to the respectable panel that - how effective do you think military cloud can be? Or do you think - will it be safe? Do you think - is it viable to connect Guantanamo with Pentagon? Thank you.

WILLIAM SCHNEIDER JR: I'm not familiar with the specific issue about connecting Guantanamo, but there is a broader issue of connecting defense operations at the edge, where the - it may not be a place where we have permanent basing, or we may not have an infrastructure. And one of the aspirations of - in cloud architecture is to be able to operate at the edge. The commander - the so-called NORTHCOM commander who has responsibility for defense of U.S. territory has noted that the homeland is no longer a sanctuary. And so there's a need to be able to operate on a global basis wherever we are - is something that's - it's not completely new. But in the data-rich environment we have, it's not something that we've been able to easily do, as our experience in Afghanistan and Iraq has shown. But I think the technology is moving in a direction that will enable us to do that, at least from a cloud perspective. There's still question marks about the communication links as to whether they will survive the fact that many countries are getting into the anti-satellite business - suggests that it may not be easy to secure the communications links that certainly have space-based links - or we use submarine cables, which are vulnerable to being cut. Yes, sir?

AUDIENCE MEMBER: Historically, the RFI - request for information - process is in use to look to industry to come forward before procurement document is completed and ask industry to provide their best advice relative to what the particular question is in terms of procurement. I believe both Dr. Schneiders, earlier, spoke about this particular procurement where they brought industry together and asked for best advice relative to, how did you deal with this? So my question is two parts. One, where is DARPA, then, relative to this whole process? - number one. And if they haven't been involved, why? And the second part of my question is, given the level of threat not just to military cloud but in terms of hacking, where in the last 24 to 36 months we've been told the director of the CIA's email has been hacked. The secretary of defense email has been hacked, et cetera - my question is, why are we not looking at this as an existential threat to the United States and going about it from the standpoint of putting together our best and brightest not for a single procurement but an ongoing basis such as we've done for the National Renewable Energy Lab, the national atomic labs, et cetera in bringing both industry and the best minds in government together on an ongoing basis such that this is - kind of question is being addressed consistently and with the best minds out there?

HERMAN: You left out one player, and that's universities.

AUDIENCE MEMBER: I said the best minds out there.

HERMAN: OK, OK.

WILLIAM SCHNEIDER JR: Well, I'm sure everyone has some observation to make, but I think the problems you cite are correctly posed. This is really a national problem. It's not just a problem of DOD, the financial services industry. All of the basic infrastructures is subject to these vulnerabilities. And the - a problem continues to make it difficult to resolve, which is the

sensitivity of the information on the threat. I believe there's a consensus that you just can't protect the assets by some sort of perimeter defense. It's a much more complicated thing. DARPA has been - done a lot of work on issues relating to cybersecurity but, in general, not cloud because I think that does not fit the DARPA notion of being a DARPA hard problem. There's a couple of hundred cloud service providers. And there's not really much they can add that has a techno nerd kind of requirement. But the security element is something that they have been working on. And a lot of the DOD and intelligence community efforts reflect that effort.

HERMAN: I was going to say - to go to your point, I think what we're seeing here with regard to DOD and cloud is also reflected in the issues over 5G. In fact, the panelists were just discussing about this earlier, the degree to which 5G has really proven to be a kind of inflection point, which is, yes, it's easy and understandable to talk about China's role in all this and the possible malign role that Huawei will play in terms of its development. I've written columns on it, for crying out loud. But ultimately, the real issue is, why can't we get our act together? And the problem of why is it that something which would seem to be very much within what American industry and government working together do, why is it that on this one, everything seems to have sort of gotten stuck - from the point of view of developing standards to the point of view of arranging - finding out how we're going to put together the infrastructure and where the investment's going to come - to put that into place - and also how you develop a 5G network that's going to be able to be constantly evolving as the technology evolves? So these are all issues. That's the real existential issue, it seems. I mean, why is it the United States doesn't seem to be picking up the kinds of - and doing the kinds of achievement that is - that its history is based upon?

FRED SCHNEIDER: Right. So I would like to enlarge the problem slightly. Yeah. So we could have software - we, all of us citizens - private citizens and defense folks - could have software that's quite a bit more secure than what we have today. It would just cost more. That is we have on - in the labs the ways to do this. It would cost considerably more. And the cost would be not only monetary, but it would be probably less convenient to use. It might change some of our values. For example, we would monitor things to detect intrusions. Well, that end has a cost in terms of privacy and First Amendment rights and so on. So there needs to be a discussion, at the level of our nations, to decide whether and how much we want to invest and what we want to get back from it. Until that discussion happens, we're not going to make real progress on this. And the - I said it's going to cost more. And the question is, who's going to pay? And you might be thinking, oh, well, the government should pay. Or you could say, well, the soft - the industry should get less profit. Or you might say that the investors should get less. But look in the mirror. Those are you. So whoever - however we apportion the cost among the participants in our society, it's all of us. And we need to come up with a scheme for doing that partitioning. But that won't happen until there's a widespread discussion, and we agree that it is an existential threat, and it is more important than - and you can list 10 other things that also are debated, like climate change. And that's the scale that this has to happen. So the JEDI procurement is not the way to get a more secure software for everyone. It's really a fairly big national problem. And as Bill mentioned earlier, there are a lot of interesting public policy regulation questions about how to incentivize investments, how to apportion it and so on. And there has been some discussion about it. But that's where this question is. And now the JEDI problem looks really sweet compared to...

(LAUGHTER)

WILLIAM SCHNEIDER JR: To the other one. Yes?

AUDIENCE MEMBER: Is there some way to have all the security on the high-end stuff that you need it on? But there are people who - just to get on the computer and trying to remember some of the passwords and use it as a - at the lower level. You've got - you know, you need to keep them in mind and sort of maybe have the high-end for all the people that are doing security stuff and military and whatnot - medical. But leave an opening somewhere for the people who are just doing emails back and forth to their grandkids.

WILLIAM SCHNEIDER JR: Sure. It's - the costs are divisible in the sense that if you don't want much security, it won't cost you much to have the little security that you desire. But if you run a bank or a hospital or a motor vehicles department, you may want more security. And the people who you serve will also want more security to the data. So those services are going to cost more. You'll end up paying more for them because you use those services. But - I don't know - French are (ph) talking about this also. Maybe you have some additional thoughts about how to apportion costs.

FRED SCHNEIDER: No, not in a short time.

HERMAN: Not in a short time.

FRED SCHNEIDER: Let me - that is to say, I did lecture for an hour last week in San Antonio on this, but it's hard to compress.

WILLIAM SCHNEIDER JR: Yeah. Well, it's a - the aphorism that you get what you pay for is - probably cuts out about 58 minutes of Fred's lecture.

(LAUGHTER)

WILLIAM SCHNEIDER JR: Yes?

AUDIENCE MEMBER: We have not discussed FedRAMP's appropriateness for the cloud security models - you know, its timeframe, you know, what its evolution is. It's a paper-based process, as you know, and it takes forever, and it costs a lot. So what do we do with FedRAMP if that's the compliance mechanism today, and it takes 36 months to get through?

FRED SCHNEIDER: So let's distinguish between two things. One is, what is the hurdle? And the other is, how do you evaluate whether somebody jumped over the hurdle? We need an efficient way to evaluate whether someone's jumped over the hurdle. And it could be easier or harder to do that evaluation depending on what the hurdle is. I think the - and FedRAMP was a wonderful early step. It was really advanced. It was way ahead of the curve. And initial efforts often need to be refined. So I think if DOD does a good job of formulating a reasonable definition of compliance, then I wouldn't be surprised if FedRAMP followed suit, especially if DOD had a good way to do this evaluation of compliance. One of the advantages in the cloud space at the scale of DOD is if there are only a reasonably small number of clouds, then you only incur the cost a small number of times. And that's much better than if we're doing every little mom-and-pop system.

WILLIAM SCHNEIDER JR: Yes, sir?

AUDIENCE MEMBER: Gentlemen, this has been very U.S.-based. Do we know where our competitors are at this time - nation-states and even lone wolves - China and Russia, lone wolves, nation-states...

WILLIAM SCHNEIDER JR: Well, the...

AUDIENCE MEMBER: ...Boiler rooms?

WILLIAM SCHNEIDER JR: The Chinese will probably make a lot of the hardware that's going to be in the 3G system, so they're a partner in some perverse sense. But...

AUDIENCE MEMBER: (Inaudible).

WILLIAM SCHNEIDER JR: Right, and I - at this point, the state of the microelectronics industry in the U.S. would not support a large presence. Perhaps over time with additive manufacturing and other advanced manufacturing techniques, it'll permit us to get back into the microelectronics business in a way we haven't been for 15 or 20 years. But Russia and China clearly are going to be interested in this. They will have their own clouds. Russia's likely to do it differently for a number of reasons. China's increasing leveraging of modern software communications and microelectronics makes it likely that they will have some of the same vulnerabilities that we have.

AUDIENCE MEMBER: (Inaudible).

WILLIAM SCHNEIDER JR: Well, they are...

AUDIENCE MEMBER: (Inaudible).

HERMAN: Data. Harvesting data.

WILLIAM SCHNEIDER JR: Yeah, they...

HERMAN: They're certainly engaged in that, as are the Russians.

WILLIAM SCHNEIDER JR: Yes, they have - and they have good skill sets. A lot of the data they can't exploit because they don't have the infrastructure for it. It's stolen. They have a process where they launder the data through some of their universities. They get - or they file patents on it in China, then parcel it out to these big development complexes that they have for the exploitation of data by their so-called national champions.

HERMAN: So what - a lot of what you're seeing right now in China in terms of investment in securing data and networks is in quantum communication. That's really where they're pushing hard and where a lot of the investment's taking place, a lot of experimentation, developing both in terms of - pardon me?

AUDIENCE MEMBER: (Inaudible).

HERMAN: Well, it's very difficult to judge. The Chinese are also very good at hyping the achievements that they do have. For example, the most recent report is that they've managed to - sort of broken the world's record in terms of cubit entanglement for a quantum computer, which may be true, although the significance of that, I think, is rather - more you know about quantum computers, the less significant that becomes. But from the - getting to the issue about where they are in terms of - they're already thinking sort of past the cloud. In other words, they're thinking about QKD and QRNG and being - and finding ways to create hack-proof communication within China itself, not for the systems they'll be building out (laughter) in terms of 5G - Huawei's not going to be engaged in that - and then, of course, also quantum satellite communication. Their launching in 2016 of the Micius satellite was, on the one hand, an

experimental, but it was pointing the way to where China assumed they'll be able to develop. So you've got a dual strategy of building quantum computer - talking about the quantum technology area - building quantum computer - right? - which could be used for offensive decrypting purposes, but at the same time, hardening their own communications sites using quantum technology in order to do that. And this is a longtime strategy. If you look at the history of patents that China and other countries in the quantum technology arena - if you go back to 2015, for example, what you see is in 2015 the United States still had a very substantial lead in terms of patents in quantum computing. That's eroded somewhat today, but a very substantial lead there. But in 2015, China was the No. 1 country in terms of quantum communication patents, so they were already beginning to sort of think that this is the direction they want to go in the future.

WILLIAM SCHNEIDER JR: A lot of the patents are based on purloined information that they reprocess and run through their patent system so they can claim national ownership of it.

HERMAN: Well, I think that's very true. But what's also true is that there's a strategy underlying all of this. And that is where they see the future for securing data and networks, their own goes in - probably in that direction.

FRED SCHNEIDER: There's another complication. Two of the very large cloud providers, Google and Amazon, are multinational companies, right? They're not in the business of providing clouds to the United States. They provide clouds to the world.

HERMAN: Everybody.

FRED SCHNEIDER: In fact, Google, which is reasonably secure, is as secure as it is because it found itself hosting dissidents and felt obliged to protect them from their countries. So it was the playpen for countries to try to identify dissidents and track them down. One of the problems with the Snowden revelations was it made our multinational companies, like Google and Amazon, suspect in the rest of the world as being instruments of the intelligence apparatus in the United States. So it's not like there are national cloud businesses in the U.S. There may be national cloud businesses elsewhere. There certainly is one in China. China has replicated Google and most of - and Amazon separately, and China has fenced off their Internet and so on. Russia talks about fencing off their Internet, and our recent antics with regard to disabling their attackers during election day sent a strong message to them that they should have the capability to disconnect themselves from us. But we really have been in the lead. And it would take quite a bit of development for them to follow us, yet we're our own worst enemy insofar as we have a business - businesses that would like to be providing the clouds to as many other countries as they can. Probably they won't get the contract in Russia. They haven't gotten it in China. And India is the other place where there's a strong sense of nationalism and a strong desire to develop their own technology so they're not dependent on it.

AUDIENCE MEMBER: I was also the DOD liaison at National Counterintelligence Executive Committee, and I ran an experiment. And what I did is I picked directed energy, not quantum computing. And I asked our Open Source Center to give me the best 10 Chinese papers on that particular domain, directed energy. And then I gave it to our leading directed-energy scientists - lasers. And I asked them to rate it for referee journals. And they culled through the 10 and said maybe three may make it. But the No. 1 problem they saw was plagiarism. It was huge. And what they saw was people with degrees that had nothing to do with the exact science they were writing put their name at the top. And they tend to stifle backward in their society in a whole lot

with the plagiarism issue. The second thing I found out is when they stole, for example, the F-35 alliance system. It was the equivalent of a student stealing maybe the midterm of Algebra 2, but the conclusion is they have to pass Algebra 3. And that really inhibited them because they didn't know the problems getting to that solution set to build off of. So they're not 10 feet tall here, but they - as the doctor said, they will steal everything they can get their hands on, including at Wright-Patt. I looked at their acquisition process, and it was they put it out. They talk about it. Then they go dark for a while. They may test it. And then they have a problem, and they go say, go steal the answer and then continue on. So the way in which they develop it is not quite the same way we do in the Defense Department. That's my experience.

HERMAN: Should we wrap it up?

WILLIAM SCHNEIDER JR: Yes, I think we're at the end of our session. I appreciate the absence of bricks and tomatoes. Thank you.