THE ASPEN INSTITUTE

ASPEN SECURITY FORUM

Emerging Technologies

Doerr-Hosier Center
Aspen, Colorado

Friday, July 20, 2018

Cecilia Kang: Emerging Technologies, The Promise and Peril.

I am very pleased to have with me, Teresa Carlson. She is the vice president of Worldwide Public Sector for Amazon Web Services. If you haven't heard of Amazon Web Services, they are basically storing the data of much of the world these days.

Stacy Dixon, the deputy director of Intelligence Advanced Research Projects, also known as IARPA. If you don't know what IARPA, think of it as sort of the DARPA of the intelligence community. She previously had assignments at the National Reconnaissance Office, the National Geospatial Intelligence Agency, and the Health Intelligence Community.

We are also joined by Congressman Will Hurd from Texas. A member of the House Permanent Select Committee on Intelligence. He is also a former CIA officer.

And we have, last but not least, Sam Visner. He's a director of national cyber security for the federally funded research and development center FFRDC, or MITRE. You guys do love your acronyms in government. And he is also a former signals intelligence chief for the NSA.

I wanted to actually start before we get into this very exciting conversation about emerging technologies, to do something awful and ask about politics. I wanted to ask Congressman Hurd about an op-ed you wrote this morning that was published in the New York Times. And let me just read one, two sentences from it. "Over the course of my career as an undercover officer of the CIA, I saw Russian intelligence manipulate many people. I never thought I would see the day when an American president would be one of them." My question for you Congressman Hurd is why did you write this op-ed? And do you see, and this was obviously probably written and submitted before the news of yesterday when we learned that the president plans to invite Russian president Putin to the White House this fall. Why did you write this op-ed, number one, and number two, do you think anything productive can come from meeting with President Putin in the United States?

Will Hurd: And I have an hour to answer this question?

Cecilia Kang: I'm gonna give you two minutes.

Will Hurd: So I wrote it one because what happened in Helsinki, to me, was an example of classic disinformation. I'm having Vladimir Putin standing up there and making some outrageous claims about Ukraine, Israel, Iran, and doing that standing next to the leader of the free world and there not be a rebuttal was exactly what Vladimir Putin was hoping to happen and in order to deal and thwart that we have to talk about ultimately these problems. The other reason I wrote it is so people know that there are things already going on in Congress to try to

address this. You know, Congress has actually been out in the forefront when it comes to supporting Ukraine. Congress has ... we just passed, out of the House, an intelligence ... the Intelligence Authorization Act, which has further money to the intelligence community in order to deal with people trying to hack our elections and our digital infrastructure. It has increased reporting requirements from the intelligence community. This is something that needs to pass the Senate and ultimately get to the president's desk.

When it comes to disinformation, we all know Vladimir Putin is ... his ability to get that message out is unparalleled and we have to be talking about this. We have to know what they're trying to do and we have to make sure that every day folks have to understand why this is important to them. Vladimir Putin is interested in one thing and one thing only, reestablishing the territorial integrity of the USSR, and he knows he can't do that militarily or economically, so he has to resort to asymmetrical warfare and that is ultimately using technology, hacking into our systems, and disinformation. So what we have to do is how do we counter that disinformation, how do we use the tools and technology available to us, because guess what, their ability to do disinformation is gonna get even harder once they get to artificial intelligence, once they're trying to get to quantum as well. So, this is a race and they're gonna use those tools to continue to do the things that they've been doing for 30 years.

Cecilia Kang: So I would assume that you are not a big fan of a meeting with him in Washington?

Will Hurd: No, I'm not because what do we get out of it, right? If Vladimir Putin wants to change his relationship with the west and specifically the United States, then guess what? Leave Ukraine. The fact that he wants to articulate what's happening in eastern Ukraine and Crimea as a separatist movement. No it's not a separatist movement. It is Russian troops, Russian tanks invaded another country. So, if you want to have normal relations, then leave Ukraine. Then turn over the 12 intelligence officers that were involved in trying to manipulate our election. There's a lot of other preconditions that should be met before you have a general conversation and we should be talking about how are we going to try to change the nature of the relationship. And guess what many other presidents have tried to change the nature of the relationship with Russia and specifically Vladimir Putin and have failed and so let's not open up that box until we have clear goals on what we should accomplish and we should have, we should make sure that they come to the table with establishing some of these preconditions or following through on some of those preconditions.

Cecilia Kang: Okay. We will get back to the topic of our panel now.

Will Hurd: I tried bringing artificial intelligence back in-

Cecilia Kang: I was gonna say, it's not so disconnected, thank you for that. I thought we'd start off with actually a little round robin, because I'm afraid we're gonna run

out of time and there's so many technologies we could talk about, and I just don't want to miss some of the highlights. Can we just quickly go down the line, starting with Teresa on the one technology that either keeps you up at night or makes you most excited in terms of its promise, or both. So just say what that technology is and say promise, peril, or both, and let's make sure to work that in, whatever that technology is in our conversation. So Teresa.

Teresa Carlson: So, you may not like my answer-

Cecilia Kang: Don't say cloud.

Teresa Carlson: But I'm gonna say cloud computing. And here's why, because it's so much promise and it's still so misunderstood. And cloud computing is so much more than one technology, clearly, but it is a basis for how you could move so much faster and so I just feel like to pick one thing out of that wouldn't do it justice because there's so many things that can be enabled because of cloud computing.

Cecilia Kang: Okay. So, cloud and promise. Let's keep it short, so Stacey.

Stacey Dixon: Sure. Synthetic biology, or engineered biology would be the one that I'd pick, and that's both, promise and peril.

Cecilia Kang: Okay. Great and we'll definitely get back to that. Congressman.

Will Hurd: Quantum computing. Both.

Cecilia Kang: And both. And Sam?

Samuel Visner: 5G because it's gonna create an entirely new cyber ecosystem around the world. One that we're not prepared to defend our interests.

Cecilia Kang: Right. Well Teresa let's continue with what you were saying about cloud. I think cloud is misunderstood.

Teresa Carlson: Very.

Cecilia Kang: It's hard to grasp. It's hard to grasp when you hear that Amazon, Google, and other cloud providers from Silicon Valley for example are trying to become partners with the government and put the government's data on the cloud and trying to understand what would that look like and what does that mean. Explain to us and maybe give us an example what emerging technologies can come about with the underlying infrastructure of cloud.

Teresa Carlson: Well in the government as an example, for years they've had a really ... it's began to be outdated in the way that they utilize technology, and thanks to our congressional leaders we do have IT modernization acts and policies going on

out there, but the US government and around the world tends to use a lot of old style where they build data centers, they replace their servers, and they just sort of wait and see what happens, and they don't have a way to experiment. And if you take the US government, 80% of the funds they spend on IT are on maintenance-

Cecilia Kang: Yes.

Teresa Carlson: Not innovation, so think about that.

Cecilia Kang: And the budget's really crazy [crosstalk 00:08:10]

Teresa Carlson: It gets bigger and bigger. And you know, the budget I would say we don't really know the number, 'cause you talk about IT and they talk about mission, and if you combine those two it's much bigger than we actually do see, but there's a lot of those funds that are actually spent on maintenance. Really what's happened with cloud computing, we came into the market in 2010. I started our business and we came in for a very kind of basic reason, which was to provide government the same capabilities that any citizen gets today through how they use technology, and the ability to experiment, fail fast, have agility, have the reduced price that we provide to all of our customers. We felt it was important and we heard it from our customers and also we were drawn in from our partner community, who said, "We'd like to see you there," so it's really picked up steam. Now they see it as the new norm, just like if you go to Silicon Valley startup, they don't know any other way. If you go to a startup in Israel, if you go to a startup anywhere, they don't know any other model except the use of cloud computing when it comes to powering their tool.

Cecilia Kang: Can you give one good example in the security field where an application, a cloud application, is being used, either by the US government or overseas, that you think is really something that could be either a ground breaking application or-

Teresa Carlson: So the one thing that we're seeing being used a lot of, and I always say our customers are the smartest, they're amazing, they take tools and technologies and really put them to work, and there's a tool called Kinesis, it's AWS Kinesis, that does streaming of live data and analysis of that live data, and we're seeing our customers utilize that tool for streaming of cyber attacks. So they can take and understand within their environment what's happening on an ongoing basis and do that real time analysis and one good example is Army Cyber Command looks at all the attacks coming into them and they have now, they're running about ... they have about 500 terabytes of data and they've identified over 5,000 attacks and now looked at countermeasures in real time.

So the thing about, I'll go back to cloud, why is it so important, because you can get real time information on an ongoing basis and do that real time analysis and there's other tools that come into that like machine learning, data analytics,

there's lots of tools, but the thing is now you can combine those and they can work together, whereas in my earlier days of tech, I'll just say a lot of these tools would not work well together. Through cloud applications, you can build things very rapidly and you can fail fast and recover fast. So when you build a tool or an API capability, you can, if that's not working, you don't have to throw the baby out with the bathwater. You can utilize what's working well and then be additive to it, you don't have to shut it down and start all over. But the tools that are being used as countermeasures I would say, analytics and countermeasures and they can also look at internal cyber activities that are going on, so not only do you look at externally what's happening, but internally because guns, guards, fences, and dogs don't protect your data anymore.

Stacey Dixon: But there is a comfort level in being able to have that fence around all of your own data, but I think in terms of being able to take advantage of the commercial offerings, the apps that are now available in the cloud that we can now bring to our data, we definitely want to increase that comfort level. We at IARPA see a world in the future where maybe one day we're actually comfortable putting the classified data in places that right now we are not comfortable putting it. And we're looking at whether or not what can we do to increase the confidence that the government has that we can all protect the data and working very closely with partners to make sure we can get to that place.

Teresa Carlson: We do have a classified cloud with the intelligence community.

Stacey Dixon: Correct.

Teresa Carlson: Which is top secret and secret, which is now you have those [inaudible 00:11:57] words within you know the different classifications and networks, which I agree with you is completely important when you're talking about intelligence data.

Will Hurd: And we should be actually talking about multiple cloud environments, not just a single cloud environment. And if anybody is not talking about transitioning into the cloud, that should not be the conversation. The conversation should be what are we gonna do, and how do we defend that and make sure that the steps, we're taking the steps in order to protect it. Because, look, this is not emerging technology.

Cecilia Kang: Right. This is today.

Will Hurd: It has emerged and we need to be taking advantage of it because of the efficiency it brings us, and the computing power it actually brings us as well.

Cecilia Kang: Well trust is a big issue here as you bring up and I know this is not directly related, but just this week on Amazon's big prime day, you had a crash, and there's also resistance culturally to working with the private sector with something so important with sensitive data. How do you breach, or actually

how do you bridge I should say the gap in trust. And I can ask Teresa or anyone else in the panel that. Between private and public.

Will Hurd: I think it starts with knowing what good digital system hygiene is, right, and so when I got out of the CIA I helped start a cyber security company, so we basically broke into banks, stole their money, and showed them how we did it. And guess what? I will always get in. And so the question is how quickly can you detect me, can you quarantine me, and can you kick me out.

Cecilia Kang: Yeah.

Will Hurd: And ultimately the biggest point of failure is gonna be people. And I will always be able to get someone to click on something they shouldn't be able to click on. And that's ultimately how most of these things happen, and it's not like zero day attacks. Zero day is a vulnerability in software that has never been seen before. Most of the major attacks that we talk about and dealt with are all stuff that we knew about, so if you patched your software, if you did those basic things, you would be able to defend your digital hygiene, so the question about trust me it's about making sure federal CIOs are doing everything they can in order to do the basics, 'cause that's gonna defend you against 92% of the attacks.

Samuel Visner: I remember going back a few years ago that people said, "Well, cloud will never be secure. I'd never put information in the cloud that I regarded as proprietary or corporate sensitive, or PII." And then we learned that's like saying, "Well, I would never drive a car, because I like my horse and buggy." So you can keep your horse and buggy, but there's no place to drive it. We're at the point now where we're gonna be doing cloud on orbit. We're gonna have satellite based cloud storage. That's happening now.

When people talk about is it gonna happen, you can look in the rearview mirror and see that it happened. People said, "Well, we won't use cloud for critical infrastructure." GE predicts C3IOT, they're using cloud analytics now to help make decisions about the management of resources in infrastructure. And I would say pretty sure we're actually gonna manage the infrastructure through cloud architectures. So the question is not are we gonna use it, but how can we use it securely. Miss the national institutes for standards and technology is doing important work on the development of an architecture for secure cloud, a reference architecture that can anchor other designs. There are tools in terms of multifactor authentication and other tools that are coming online that make these things secure. So I think the challenge for us is not to say, "Oh my God, how do I protect myself from the cloud," it's "How are we gonna protect ourselves properly." And one last point, people used to say, well I'd rather protect information on my laptop than in the cloud. So, the laptop you haven't patched, doesn't have a firewall, could get stolen, that you let somebody else in your family or your office borrow, you mean that laptop? That's the one-

Will Hurd: The password's password.

Samuel Visner: No, password123.

Will Hurd: My bad, my bad.

Samuel Visner: Well that can make it confusing, so I think cloud represents actually a strong opportunity to get it right if we're not sloppy and we're not lazy and we do get it right.

Teresa Carlson: And I, speaking of outages. I can tell you that the government everyday experiences massive outages in their data centers, but the great thing that's happening now is there's transparency when things happen. So afraid of, yes, but of course we've had glitches where we've had some outages, but we're so transparent about it. And the thing that I love, when you're a builder and you run toward hard problems and not away from them, you can learn a lot from those things and if you look like we're very open, anytime there's been an issue, we always do what we call a COE, or root cause of analysis, and you can go to our website and we will tell you everything that happened and what we're doing about it and we always come up with innovations as a result of those kind of problems. And I'll just go back to if you could move faster and have agility and learn from those glitches and move forward, you can't hide, you can't run from the things that are happening, you have to be open and transparent with your customers, you have to build trust.

And back in the early days, I remember I would walk in, when I started this business, I would go in and they would say, "No way, no cloud. You're not secure. It's never happening," but now, today, I would tell you that the primary reason people are moving to the cloud is because of security. And the things we're talking about. The ability for visibility, analytics, tuning, looking at what's actually coming to you. That would not be possible today in data centers that are sitting there that are improperly patched or used.

Cecilia Kang: So the cultural change has happened.

Teresa Carlson: Yes.

Cecilia Kang: And Stacey, I do want to get to a different kind of cultural issue, and it comes down to norms and you mentioned synthetic biology. First can you explain to our audience, what is synthetic biology? What is the promise and the peril, if you will. What are your concerns as you look at it, and how is the US researching and developing synthetic biology vis-a-vie other countries, such as China.

Stacey Dixon: So synthetic biology is the ability to take the genetic pieces, or DNA, and put them together in different ways to come up with organisms that do not naturally occur. And we've seen it in simple ways like being able to edit the genome to be able to target specific diseases that perhaps we were trying to prevent a child from having. We've seen research like that talked about overseas and we're getting closer to the place where the US may be interested,

well we've done research in it, but in terms of actually putting it out into use, it's still a very difficult conversation to have because we're still trying to understand the implications of if you edit a piece of the genome, do you understand what's going to happen in the rest of the genome, do you understand all of the unintended consequences. That's the good use, to be able to help diseases. To be able to, take for example, to focus on the mosquitoes that carry malaria, and to be able to make them sterile so they cannot reproduce. That is something that was contemplated.

Having said that, on the other side is, you can use the same tools to be able to put in pathogens, toxins, productions of things that would cause harm. That if put out into the wild would be very dangerous to people, animals, agriculture. And there's the balance of the good things you can do with synthetic biology, bad things that you do either accidentally, such as bio error, or the things people do on purpose such as bio terror.

Teresa Carlson: Like the fly? Remember the fly? Where the guy got in with the fly? [crosstalk 00:19:31]

Cecilia Kang: Is the US thinking about this balance? Are other nations as hesitant, do they have those red lines? And what does that mean for this emerging technology and our security going forward? If you could be specific.

Stacey Dixon: Absolutely. So definitely I would say the US has a very high value standard when it comes to this. We're often the ones that are saying, "Let's be careful how we enter into using genetic engineering. Let's figure out what the norms are that should be used across the world." We are very hesitant to use it for example, for cosmetic reasons. You're not gonna just go and pick the color of your child's eyes. You're not gonna pick their height. Just because that's choices we've made. There are other places where picking those things, trying to give your child an advantage through genetic manipulation is perfectly acceptable. Or at least doesn't have the same sort of reaction as it has, if you talked to a group of Americans.

When it comes to research, it's sort of the same thing. There's certain things we're going to enable our researchers to do here and other things that we're going to encourage them not to do, partially through the government funding that's not going to go to certain things. And there are other places where people can go and continue that research and it's going to be a challenge. We're going to have to figure out where we continue to stand in leading in the sort of moral situation where we want to make sure that the values that we're putting forward in our science are the right ones, but if other countries are going forward and trying these things out. A, we want to make sure that they're doing that, but B, what do you do and how do you compare-

Cecilia Kang: How do you even know what they're doing, if you can't research yourself?

PART 1 OF 3 ENDS [00:21:04]

Cecilia Kang: How do you even know what they're doing if you can't research yourself?

Stacey Dixon: Thankfully, there's a lot of publications right now, but I imagine there will be other things that people will not publish on, and then we'll have to use other means to learn about what's happening.

Cecilia Kang: Congressman Hurd, can you talk a little bit about Quantum? Explain for our audience exactly ... just define fully, and you've talked a lot about this in opinion editorials as well, about the promise and the peril of quantum computing from a national security perspective.

Will Hurd: Sure, so currently in computing a bit can be a one or a zero, okay? And then you string a bunch of those together to do a if than. Like, if this thing happens, then execute here. A quantum means a bit can be a one, a zero, both or neither or all the above, all right? And to me that's like a crazy Scrodinger's cat, right? It is a ... thanks for the one philosophy major in the crowd that laughed.

So what that allows you -

Samuel Visner: Can't find that cat.

Will Hurd: Yeah. What that allows you is in a simple way is the power you get from being able to do that is incredibly significant which means ... and an example is, whoever gets to true quantum computing first, will be able to negate all the encryption that we've ever done to date. That is why China, that is why Russia, is sucking up cipher text.

Cipher text is you have whatever your piece of information is, you encrypt it. That encrypted data gets transported. And it's in the air, you can pick it up, but you don't know how to read it because you don't have the key to decrypt it. So what Russia and China are doing is they're sucking all this cipher text up because once they achieve quantum, they're gonna be able to break that and read everything going backwards.

So that is ... Quantum's gonna get us to a point where we have to rethink encryption. But a positive is, quantum's gonna be able to do some molecular modeling that we can't do now that is going to reduce the amount of time it takes to bring medicines to the forefront. Another more basic example is driverless cars. To achieve true efficiencies with driverless cars, you're gonna have to have all the driverless cars talking to one another and right now the best algorithms, the best computers can do maybe 500 vehicles, right? That ain't gonna work in NYC or Tokyo, right? And so quantum is what's gonna allow us to have the computing power in order to achieve that type of issue.

Another example, Fort Davis Observatory's in my district. It's the third largest telescope in the world and they are looking at trying to categorize one million exoplanets. An exoplanet is a planet outside of our solar system that could potentially support life. This is a data problem. And so we do not have the computing power to analyze that kind of data. So that is another thing and I think quantum's going to be able to help us achieve it.

Cecilia Kang: So how's Washington thinking about quantum? We're really great at looking back. At this conference there's a lot of talk about social media and interference still and that's kind of looking back like, "Wow, we now know what happened in 2016." I've heard that quite a bit over the last few days.

There are so many things, not even just around the corner, like within sight. Is Washington -

Will Hurd: So there's probably four members of Congress talking about it and three of them are here this weekend, right? Darrell Issa from San Diego's probably in the crowd here somewhere and then also Chairman Mike McCaul from Austin, Chairman of Homeland Security and this is something he's thinking about. But the fourth person would be another Texan, Lamar Smith who just put forward a proposal to establish a national coordinator for quantum computing within the White House to kind of drive a strategy on how we do this in order to focus investments from the Federal government and to be working with the right folks in the private sector in order to achieve this first.

China is doing ... with China this is one of the areas that by 2049 they're trying to become the world leader in, and I would say right now it's tied. And this quantum coordinator is similar to what we did in nano technology. Probably about 15 years ago there was a coordinator in nano technology in order to drive this and it's did it job because now every industry that does something with nano technology has started to do more advancements. I'm in that area.

So that is probably the best piece of legislation right now in Washington. But when you look at the executive branch, NASA Science Foundation, they're doing a lot of efforts in trying to do some of the basic science but ultimately we need increase the amount of basic science that's happening in the Federal government.

Cecilia Kang: And Sam, is there the leadership in place, or is there leadership on these issues in the way that there needs to be in the US. And I mentioned this and that you can't talk about what's happening in the US in a vacuum when China has a made in China 2025 policy and they have what is essentially kind of a taboo word in the US of an industrial policy on this. And a lot of people feel quite uncomfortable with that. What is your thought on the policy and leadership and coordination within government?

Samuel Visner: Well let me answer that question by first giving an example and then making a somewhat more general observation. I think you ask, what technology do I think is exciting but also keeps me awake and I said 5G. And in comparison to synthetic biology and quantum and all the other stuff, it sounds like going down to the bus depot and watching paint dry. 5G what is that?

But as 5G is developed, it's going to create a tremendous opportunity. It will change the nature of the entire cyber ecosystem around the world. It will mean that the promise of IOT in critical infrastructure and other devices being connected directly to the internet without intermediate networks. Being able to take direction from and send data to the rest of the internet. That's going to happen.

Cecilia Kang: And just quickly, what is 5G?

Samuel Visner: 5G is the fifth generation of the internet, but instead of it essentially the internet being parceled up into the part that your phone uses and then the other devices in your house, there will be large-scale general networks to which everything can be connected at very, very high speed.

This will change fundamentally the nature of the cyber ecosystem. We talk about using machine learning and artificial intelligence. We will now be able to unleash those technologies on infrastructures that are much more connected, much vaster than they were before. That's great.

Now here's the part that worries me. That ecosystem is being built not essentially on hardware built in design and built in the United States but by three countries, two of which are in Europe and they're smaller and one of which is in China. So the companies that are building the infrastructure of the next global cyber ecosystem are not US firms. One of the them is a Chinese firm.

I'm not saying it's a bad firm but it means that we are going to be living in a ecosystem of cyberspace that is essentially not an ecosystem that we can manage, that we can control. And let's take a look at what China thinks about cyberspace. We look at it as a global commons. China looks at cyberspace as sovereign territory. For them cybersecurity is not about safeguarding Congressman Hird's information, it's about regulating human conduct. And if cyberspace can be treated as sovereign, it can be conquered, it can be controlled and it can be governed. And that is the global infrastructure that's going to be created and the question is, is somebody else gonna regard it as sovereign?

Now to answer your question at a more general level, the term industrial policy is a hard term but if you go back to coming out of the second World War, we mastered and dominated nuclear technology. We mastered and dominated aerospace technology. We got people to the moon and back which they probably appreciated very much. We did so by building up coordinated

strategies of government and industry and academia that had White House leadership, that had national strategies with national goals.

The idea that there would be a quantum coordinator who could drive the development of a national quantum R&D community and then help that community build a whole of nation strategy that involves government, industry, academia, is essentially whole of nation. That's the right thing to do and I would encourage the administration to undertake that kind of thinking. Because if we are going to predominate or at least hold our own in these advanced technologies, we're not gonna be able to leave it up to chance and we have to decide that the high ground in those technologies isn't just a market imperative, it's in the national interest and should be treated as issues in the national interest.

Will Hurd: One of the things that is common in all that we've talked about is the United States has to show leadership on this. Because if we want these new things to evolve in a way that is good for freedom loving people everywhere, we have to show leadership on this.

Cecilia Kang: So absolutely. Is the United States showing leadership from the top of the government? From the White House? The White House just eliminated the cybersecurity coordinator role. We're talking about the idea of a quantum coordinator role. We just eliminated the cybersecurity role. Where is leadership? Is there leadership?

Will Hurd: Michael Kratsios who runs the science and technology, he cares about these things. He's working on these strategies. You have individual folks in Congress and you have Congress directing resources. When it comes to artificial intelligence you have money that has been put aside.

So can it be more coordinated? Absolutely. But it is happening. There are elements within the executive branches doing it.

Now the one area that I think was a terrible move was getting rid of the Ambassador at large for cybersecurity out of the state department. Because even now, every country doesn't have criminal laws when it comes to hacking. And so our diplomatic efforts in that area is important. And so can we always show more leadership? Absolutely. Because the technological change we're gonna see in the next 30 years is gonna make the last 30 years look insignificant. And if the US is not playing that role in driving with our allies on these issues then China's gonna get there.

Cecilia Kang: I think there's absolutely agreement that there needs to be leadership. I think you find that within this room. But there doesn't seem to be agreement on what to do. And what I mean by that is, I mentioned this pause on the idea of 5G, Sam. There was a paper that was leaked from the National Security Council

about the idea of a Nationalized 5G Network and that paper was roundly ... was very controversial.

The private sector, tech companies, a lot of people within the government thought that the idea of government running a mobile network for the future was not a good idea. So there's not even agreement.

I mean that was not necessarily ... It was a paper. But it was not necessarily something that the White House had baked and was ready to propose, but it was ... it showed how divided and how there is not agreement within the government.

Samuel Visner: Well, look. Two things. First, whether or not we're divided or united, let's take a look at our ... a lot of debate over competitor, adversary. Let's take a look at our peer competitors.

They have put in place strategies that have goals and benchmarks. They know what they want to achieve. They know by when they want to achieve it. They've put together the resources that they're mobilizing to achieve it and they actually have a plan. Do we? I don't know that we do. So one of the benchmarks might be to see at least what other countries believe a plan looks like.

And the second thing is if we don't know what a plan looks like, we can look to our own history. When I take a look at the Manhattan Project. When I take a look at what people like Rickover did to build nuclear energy into the Navy. What others did to build commercial nuclear power in the United States. What others did to essentially get us to the moon. We mobilized with real plans. To me, those are excellent benchmarks. Those are excellent standards against which we could build national strategic approaches. And to be quite candid I don't think we've quite done that yet in some of the technologies that have been outlined here. Whether or not we should, others may judge but I think we should. But whether or not we do, we shouldn't fool ourselves; other countries are approaching it from exactly that perspective and they took a look at the model that we used to make ourselves successful and they've adapted that model and we want to consider doing the same.

Cecilia Kang: One key difference -

Stacey Dixon: We definitely need a plan. Let's just say we did have a plan. We have a lot of companies and a lot of people out there who are unwilling to cooperate and work with the government.

Cecilia Kang: Yes, yes.

Stacey Dixon: Very technical people who's skillsets we need, apply to National Security who are unwilling to work with the government. We need to figure out how to bridge that gap because we need that talent.

Cecilia Kang: This is a very important point and Teresa I want to ask you about this. They're one difference between what's happening in China and other nations compared to the US is there is no daylight between the private sector and the public and the government in many ways.

Stacey Dixon: Well the private -

Will Hurd: The private sector doesn't exist, right? Like so it's an extension of the Chinese governments, right? And so we have to be careful about some authoritarian, top down approach. The United States will always out-innovate. The United States will always come up with more interesting ideas. And we have to create a framework to allow this stuff to grow. And it may not just be a plan on by this date we'll do this. When the [inaudible 00:35:15] that did the self-driving car test or the [crosstalk 00:35:19]. The first car that won that prize only drove seven miles. Last year when this happened, everybody completed the track which was like 750 miles. That's a way that the government was showing leadership on an area to say, "Hey, let's create some objective that we can hit and see what happens." Because we may not always fully understand in graphs the second or third order of facts of some of these technologies and where they're going.

Stacey Dixon: And there are a lot of great prize challenges that the government is running that are still out there, so please look for those too.

Cecilia Kang: Teresa, what is the status of the relationship between these companies, including your own and the government? And what I'd like to mention is there's obviously the interest from the executive level in the companies cooperating. Obviously Amazon is going full in on trying to put the whole government on the cloud, if you will.

But then you have a lot of employees. Culturally, there's a gap. A lot of employees are resisting this. You saw this with employees at Google, with their involvement in a defense contract known as Maven. You saw that with shareholders of Amazon with the facial recognition software known as Recognition uses for law enforcement and their protest that there are people that work within your companies and invest in your companies who just don't want you to be involved with the intelligence community.

Teresa Carlson: Well, couple things. One is, we have over 500 thousand employees. And the greatest thing about that is that our employees all have a voice. They all have a voice and we love that but the one thing, we're committed to our customer. And we are unwaveringly committed to the US government and the customers we work with in government around the world. And we believe ... you know there's so many things that I just heard just listening to everybody here, because if you think about all these initiatives that we say government should be doing, if we don't get the skills in place, we can have all the initiatives we want but if there's no skills to do anything with these technologies we're in trouble.

and today what we see is the massive skills gap. Massive skills gap. Not just a little one, massive. And fact to the point, over at Amazon we have our own internal machine learning university because we still haven't found that there's any group that teaches machine learning as well as we teach it. So we're out now trying to work with universities and groups to actually make sure that those skills are out there. 'Cause we're talking about ... When we get into these technologies, you're talking about complex skills that are required. And so we just launched a two year program with Northern Virginia Community College which is the second largest community college in the US for a two year Cloud computing certification. The classes will start in the Fall because we're like, "We gotta do something."

And actually, President Ross, they first launched a cybersecurity program and they went from like 50 student to 5000 and they based the program on NSA and DHS standards. So we combined that. So we've got to get busy in the United States with the massive skills gap. And I do think the US government at all levels could really help. We gotta pitch that. At every individual district level, from all the way up and down, to every parent sitting in this room. We should not be okay with sitting back and not ensuring that our schools are teaching the right skills. So that's number one. That's job one for us at every level, is skills.

The second one, when it comes to ... I'll go back to your question of ... employees need a voice. You said, "Hey, do people want to work with governments?" Well I can't speak for any other company but we want to work with our government. We feel compelled ... I went back to where I started is that we believe the government should have the same capability, our war fighters out there in the field, our civil servants, should have those same capabilities. And government should consider commercial more than building it on their own. I mean I think one of the things we're getting into that we've got to get to the point where government has the ability through the right acquisitions to move fast, just like a startup does in Silicon Valley. And today, it's hard. I mean we're a big company but let me tell you, we had the tenacity and grit to stick with it because it's not easy.

And when we went after and we decided that we were going to bid the intelligence [inaudible 00:39:45], that was because we heard from the customers they wanted us to bid it. And we made a decision as a company that this was a really important space that we thought we could help. And if you look at tools like recognition as an example. We've got to make sure as a nation, people should have a voice and tools should always be used ethically. We need to make sure that ... you're always going to have bad actors. But recognition is such a great tool and it's being used for such amazing things.

Let me just give you a couple of examples. It is being used today with one of our partners called Thorn which is a small not for profit that started with one goal; find children who are being sexually exploited. And they have a tool called Spotlight that uses some of our AI and is now using recognition to go on the

dark web and look for these children. I mean this is like horrible y'all. And every day ... think about individuals in the law enforcement arena trying to go in and look at these things and finding these children that are being sexually exploited. And if you can use AI and machine learning tools to automate that process through recognition of children, that's a good thing. And today we've identified 21000 individuals, 6000 of those children. And we're working with law enforcement officials in the United States and Canada.

There's a homeless project we're working with in Washington state where it's a self-identified program where we work with the Sheriff's Department in Washington state, Washington County, to go in and look for ... the families come in and say, "We want to sign up our children with disabilities or an elderly who may have dementia or Alzheimer's," so that they can look for them if they were to get lost. So there's programs like that that are working.

Cecilia Kang: Has Amazon set ... drawn any red lines? Any standards, guidelines, on what you will and will not do in terms of defense markers?

Teresa Carlson: Well we have ... in terms of what work?

Cecilia Kang: Anything related to defense.

Teresa Carlson: We've not drawn any lines there because like I've just said earlier we are unwaveringly in support of our law enforcement, defense, intelligence community and that's just ... when you're working with those you can't really say ... we provide them the tools -

PART 2 OF 3 ENDS [00:42:04]

Teresa Carlson: ... working with those, you can't really say. We provide them the tools. We don't build the tools they're utilizing. We provide them the tools. We don't provide the solution application that they build. We often don't know everything they're actually utilizing the tool for, but they need to have the most innovative and cutting-edge tools they can. We cannot let our adversaries have better tools than we have to defend our nation. I think that's where we stand in terms of the right tools for the right job when its necessary.

We have ethical use rights. When the government signs up with us, they still have to have ethical use rights of our tool. Obviously, if they're breaking the law, they're doing something, we would pull that for those reasons. They sign up and they know the use rights of our tools as well.

Cecilia Kang: Right. I think we have some time for some questions. Just raise your hand. We have some people with mics. Just let me ask Congressman Hurd to comment briefly about this Silicon Valley/Washington gap if you will.

Will Hurd: There's a meme going around where it's like somebody in Silicon Valley saying, "How come the first 30 seconds of the conversation in Silicon Valley is where do you work?" It's like that's exactly what happens in Washington D.C. I actually think the divide is not as big as most people are making it out to be.

Silicon Valley is such great innovation and an innovation engine for the rest of the country. They need to understand how to help educate members of Congress and the government on regulatory issues, on how these tools could be used in the future, and also to educate people on what can you do with the existing tools. I go to the whole FBI versus Apple debate when it comes to encryption.

I am a proponent. I'm for encryption. We should be strengthening encryption, not weakening it. When it came to that one iPhone, when they finally cracked it, guess what? There was nothing on it that the FBI didn't already get because they didn't necessarily understand what all the different pieces of information they could get in other ways.

Cecilia Kang: Right. The consequence was a lot of mistrust after that though.

Will Hurd: Sure.

Cecilia Kang: It drove the wedge further. Let's take some questions from the audience. Have one over here, Jim.

Murray S.: I'd like to get back ... Murray [Sullenberger 00:44:30] here ... get back to something Ms. Carlson touched upon. Science, technology, engineering, and math. None of you can function without the people you need. Our education system is in shambles. More important than that, we have people, universities. Now, I understand in IARPA there's clearance problems but even that can get around. These kids graduate from some of our best universities in the country. They can fill that STEM area. They can't get Visas.

I'll end with one little story, has to do with Microsoft. Many, many years ago Microsoft wanted to set up a center for R&D. What they did is they got 600 Visas for youngsters. There were foreign among all of them that they needed. The United States government said, "No." So, they went 70 miles north and set it up in Vancouver. Would you please discuss what I consider to be a very bad situation in this education of STEM?

Will Hurd: I'll start there. It's nuts. Right now, you have 3.8% unemployment in the United States of America. That means that you need people from agriculture to artificial intelligence and that there is a third of the kids that are in advanced degrees in the United States are foreign-born and they're having a hard time being able to stay here and use those skills.

What we doing, the Chinese kids, we're sending them back to China and now they're working for Chinese military, things like that, when we could be taking advantage of that right here in the United States of America. It makes zero sense. It's 2018. We could have an immigration policy that is based on market demand and get in the resources and training that we need.

We also need to make sure ... A scary stat in Texas, two years ago, only 2,100 computer scientists were produced from Texas University. That's crazy! There were 45,000 jobs in Texas that required some kind of computing that year. We're not producing enough people and part of it is we're not getting kids exposed to computing early enough. That's why I think we have to start introducing it in 7th and 8th grade at middle school in order to increase that throughput.

The problem? There's not a computer science teacher chilling at a Starbucks waiting to get tapped on the shoulder and be like, "Hey we've got a job for you." We have to train current teachers on how to introduce this and to me, for this current generation, coding is going to be like typing for my generation. If you don't know how to type, you're not going to get a job. If you don't know how to code in the future, then it's going to be difficult for you and that skills gap that Teresa's talking about is going to continue to expand.

Cecilia Kang: More questions. We've got one right over here. Way over here. Sorry to make you run over there. While Mike's going over there, I completely agree. Even in a [inaudible 00:47:38] space like intelligence, there's research that can be done at unclassified levels. We actually use researchers, we leverage them for our projects all around the world, so I'm all about using the talent where it is.

Emma F.: Hi, Emma [Fagow 00:47:51] New America. All of the technologies mentioned today raised some really interesting ethical questions which were gestured at. Sometimes in those discussions, you hear some like, "The American people really need to have a discussion to figure out what we're comfortable with, to set the rules of the road." Then, often we move on from there. While I totally agree that it could be really dangerous to make consequential decisions without public buy-in, I literally have no idea what the logistical infrastructure of a public discussion of these issues would look like.

I guess I have two questions. One is, what literally would it look like? Do we have the infrastructure educationally with other media channels to come to a consensus, to set rules of the road in the country the way it is now? And, in the absence of that kind of infrastructure, how do you think those consequential decisions are actually going to be made?

Cecilia Kang: Sam, can you take that?

Samuel Visner: I want to talk about that for a second. I want to make two points in one. First is, I think you're absolutely right and it's a critical issue. Look, cyberspace is not just

a place where things happen. It's not really separate from physical space anymore. Other countries are building policies and doctrines that couple what they do in cyberspace to what they do in every other domain.

It's important that we come up with the mechanisms to develop good ethical considerations. And, by the way, if not our country, others may try to dominate that discussion. As it happens, I'm sort of an American exceptionalist about this. I think we'd actually do a better job than many other countries.

In terms of whether or not we have that infrastructure, I don't know. I teach as an adjunct at Georgetown. You may have heard of that school. I teach the Cybersecurity Policy, Operations, and Technology course. I'll tell you. My students, every year, are interested passionately, not just in the technology not just in the policy, but in the ethical and moral considerations. They want to discuss it. I don't have to press them to do so.

I think in the United States there's a hunger to have that conversation. I'm glad that there is and I'm glad that it's here because I think that if this country has that conversation, we can actually lead the way in thinking about the ethical issues, in beginning to establish some of the international norms and then, assuming we have an interest in doing so, in trying to get those international norms adopted by the rest of the community.

As for whether or not that infrastructure really exists, I would turn to you and say, "We need ideas to create that discussion and to create a more general level of that discussion in the United States." So, I'm looking to you to get that done since you're younger than I am.

Teresa Carlson: Can I just say also that it's important? We actually need groups to start ... I saw this over the years. I've been in tech now for a long time and it was easier to do this when you're only releasing one or two technologies a year because in old school ... Now that you have tools like cloud, we launched over 1,700 new services and features in 2017.

There's a lot of technologies. The innovation cycles are so crazy and it's not just us, it's all these companies in here. We got to have groups actually that have these kind of conversations because the only way you can drive real change or movement is by letting people at least have a voice and have the dialogue and say, "What could work?" and actually bring to bear the good case studies of things too. A lot of times people leap to the one bad thing instead of saying, "Well, hold on a minute. How do we actually also really use all these technologies for good?"

Like we said, we're all here at a cyber conference. There's going to be bad actors. So, we got to figure out how we can segment those and really use the technologies in the best possible way.

Stacey Dixon: Some of the really good conversations do take place because academia is pushing forward. The National Academies does try to bring together, especially in the human genome editing conversation. Then, there are these international conferences where academia industry go and try to hash out these, but then once the guidelines are posted, making sure that there is that dialogue that continues where people in the American population can then be part of it too. That's the piece I think we haven't done as well on.

Cecilia Kang: Right. Right, right. More questions? There's one in the far back.

Scott Sweetow: Hi.

Cecilia Kang: He's got it.

Scott Sweetow: Scott Sweetow from the Terrorist Explosive Device Analytical Center and I have a question primarily directed to Ms. Carlson and Representative Hurd. It's been fairly widely reported that weaponized drones are being used in the Middle East and they've also been used in Mexico by the drug traffickers. Looking at a technology like drones, which Amazon has already indicated they would like to use for package delivery, and taking Secretary Nielsen's comments about the lack of laws that might govern such things, how do we better reconcile these emerging technologies, which have already been weaponized and make sure that our laws keep up with them?

Cecilia Kang: Yeah, good question.

Teresa Carlson: These are about laws. You take that one.

Will Hurd: We have difficulty passing ... We haven't passed a law on breach. There are 47 different breach laws in the United States on something as simple as what should be done if someone steals your information, right? The debate right now around laws and rules and regulations around drones is being driven in the conversation on the FAA reauthorization. That's not detailed enough to get at to your point that you're talking about.

We need our military planners who are seeing this in places like Eastern Ukraine to give some suggestions on having seen it done, what should the response be, how should we be ultimately dealing with this? We don't know enough about how the narco trafficante's are using this in Mexico. We talk about drones in the air, there's drones in the sea as well too, and that's a conversation that I don't think in a year and a half I've ever heard anybody in an official capacity bring that up.

The short answer is I don't know. The longer answer is, we need to make sure that the people that are setting these policies ... The problem is, they don't understand it enough in order to make a rule or law to govern it. Probably one of the most important entities in the federal government right now, it MIST

because this is a group that is pretty well respected by so many different industries and within the government to come up with those standards and those objectives, we should be achieving.

Cecilia Kang: Teresa?

Teresa Carlson: I can't address our drone technology because I'm not a drone person, so I'm happy to get you in connection with that person or that team, but in general, the thing I would say that you just highlighted is back to the point that, and Representative Hurd just said, is we've got to keep up as a nation with new technologies in terms of policy because even if you're creating policy in acquisition and use, it's important.

Because right now, what's happening is innovation is so rapid that the U.S. government cannot keep up with what's actually occurring. So, we have to figure out how we fill that gap up. I don't know the answer, but we need, I think, some kind of forum. We've talked about this actually in the past. Some kind of forum with our congressional leaders on what can we do to actually bring to bear forums on innovation counsel where we could, as companies and groups, come together in Congress and say, "Here's the things that are going on rapidly." So be ahead of it versus always behind it, is, I think one of the things you're talking about. Let's get in front of this versus being behind when it's already happening.

Cecilia Kang: Great. I think we have time for one more question. Is that right? Right there.

Justin Gerard: Thank you. My name's Justin [Gerard 00:56:07] from the University of Notre Dame-

Teresa Carlson: Yay! I like that.

Cecilia Kang: Did you go there?

Teresa Carlson: Nope, but [inaudible 00:56:09].

Emma F.: ... and taking the point of STEM education and taking it out a little bit further into a technical person's career and myself, as someone studying computer science and public policy, can see this eventually being a reality for me. After spending an entire education and career building a technical repertoire, or the alternative when we have people spending that same amount of time just making inroads in the policy community at D.C., what is D.C. and policymakers in general, are they thinking about creating opportunities for these technical personnel to then rotate in to this policy-making circle without pulling them out permanently?

Will Hurd: Look, I wish we were able to pay our staffers more because what we need, we need people that have actually used these tools and understand these tools to

help be advising the members of Congress. We need the professional staff at the various committees, Energy and Commerce, Homeland, things like that, that have the experience that you're talking about. The problem is, we're never going to be able to be competitive at a price point for those folks. That's why a lot of times you have ... I'm drawing a blank on the ... the fellows from various entities that come in and provide that guidance and that experience to those committees.

How many of you all watch the Senate hearings on Facebook?

Teresa Carlson: I did.

Will Hurd: Right. You mean the information's in the machine? You know? That's what we're ultimately dealing with and we actually need more members that are converse in these technologies. We need more staffers that are there. And, guess what? If you have an opportunity to go make two or 3X in the private sector versus coming doing that, working as some staffer in Washington D.C., I can tell you what 95% of people are ultimately going to do. That's why these associations are so important to have this input into the conversations.

Stacey Dixon: But, there are opportunities for technical experts in government to participate in working groups where the policymakers are listening to them and you can influence things that way as well. These are great partnerships as well.

Will Hurd: I will say this. Members of Congress, House and Senate, recognize the problem. They also understand their limited understanding and so they're actually looking for folks to help educate them and make sure we're making better policy.

Samuel Visner: This growing recognition that it's important. Look, there are what? 3.7, 3.8 billion people now in the world who have internet access. So, if you're interested in governance, and you're interested in policy, and you're interested in the public interest, and then you say, but I'm not interested in technology, in particular, I'm not interested in information technology, that's crazy now.

What I would say is that it doesn't have to be an economic incentive. If you are interested overall in the question of governance and policy in this world, and you have a technical background, you need to consider a term in the public sector, somewhere, maybe working on the Hill, maybe working in the executive branch, MIST, to which the congressman referring. That's a good place by the way. These are good places for people with technical backgrounds to maybe bring some policy smarts to the discussion because we surely could use it.

Cecilia Kang: I will end with saying thank you, but also a data point. Google is hiring AI professionals, AI academics at seven-digit salaries, high seven-digit salaries starting. So, that's the challenge. That's one of the big challenges.

Will Hurd: What's a seven-digit salary? Right? That's the problem.

Cecilia Kang: It's far ... Exactly.

Teresa Carlson: Think about it. If there were so many resources out there, there would so many, that's the new norm. That should be the new norm that all these students graduating have these skills.

That's just of an example of you shouldn't ... We want the economy to have high-paying jobs but we need just a lot more of them.

Cecilia Kang: Certainly. Right. To make the pipe bigger.

Teresa Carlson: Yeah.

Cecilia Kang: Thank you so much to my panel. Can you show some appreciation? Thank you.

PART 3 OF 3 ENDS [01:00:30]