Speaker 1: 00:55 [inaudible]. No, it's got to get him.

Speaker 2: 00:57 Alright. Good morning. Ready for our next panel. Uh, good morning. My name is Alan esterase. I am with the, I am with the Lloyd's Defense Security and justice sector. In a previous life, I was the principal deputy under secretary of defense for acquisition technology and logistics where I had the great pleasure of overseeing DARPA and the lab infrastructure of the Department of Defense. The reality is that while the Department of Defense has a great rd infrastructure, the Department of Defense relies on partnership and access to technology produced by the commercial sector in order to sustain its overmatch. And in order to deter and defeat potential adversaries, the department of Defense has to have that access. In addition, it's not just going to be the kinetic weapons that were used to in the previous, uh, wars of missile ships, tanks, airplanes. It's going to be ones and Zeros that win wars. So I think this is a very important pal for us to, to listen to. I'm pleased to introduce Keller Swisher Co founder and editor at large of recode. She has been called Philippian Valley's premiere journalists. Kairos also producer and host of the recode decode and pivot podcast, co-executive producer of the code conference series. She has written in the Wall Street Journal and the Washington Post and is the author of several tech related books. So over to you, Kara for this great panel.

Kara Swisher: 02:36 Thank you very much. So, um, I want to get started. We are going to talk about a wide range of things because I think one of the things that's, uh, important is to consider the role of technology has been brought up in a lot of panels along the edges. I'm coming from Silicon Valley. It's pretty clear that most of the technologies being used are going to be critical in the years ahead and have already been, uh, to start with, um, even just this week, um, with the freak, the national freak out over the face app, uh, which apparently Vladimir Putin is trying to steal American faces. Um, I don't know why, but he is, it's very dangerous. Um, it is actually about the bigger issue of, of these, of the, of the ongoing global, uh, cyber war, um, in lots of ways. So we're gonna talk about a range of issues and have each of them introduce themselves and you know, we have to talk about the, the players, what the u s needs to do, what it's not doing, uh, the talent, uh, the talent necessary for what's coming and what the big technologies are going to be that, that everybody needs to pay attention to.

Kara Swisher: 03:38 Yesterday the admiral talked about the idea, uh, that this is, this investment needs to be ongoing, uh, very critically, uh, noting that China would probably surpass us the minutes militarily, especially in the technology sector with by the mid century. I think that's what he said. Um, they certainly are already doing that, uh, commercially, uh, uh, in a lot of areas including AI, automation, robotics, and some critical areas. So we're going to talk about talent and where it's going. Um, why don't you have each of you introduce yourselves to explain this very diverse panel of white men in blazers here. Um, which makes me feel comfortable that I'm in silicon valley, except it would be t-shirts. Anyway. Um, please start.

Michael Brown: 04:20 Okay. I'm Michael Brown. Uh, today I'm the director of the Defense Innovation Unit, which is headquartered in silicon valley, but with offices in Boston, Austin, and in d c and I spent, uh, almost my entire career in the private sector, CEO of Symantec and before that, CEO of quantum

Michael Brown: 04:37 great. And Tucker Bailey. I'm a partner with McKinsey and company in our Washington DC office. I help lead our cybersecurity practice in North America and I also serve the Department of Defense and the intelligence community. Uh, I'm Edward scribing. I'm Oracle's chief corporate architects. Um, I, I provide a direction across, uh, all the engineering and technical work that we do. Um, uh, oracle labs reports to me. I have, um, various parts of the engineering organization working for me and I'm in charge of security at Oracle, both, both our internal security and our product that our product security assurance.

Kara Swisher: 05:10 All right. Why don't we start with Edward? Um, oracle does an enormous amount of business with the government and provide systems and things like that as given, why don't you talk first about what you think right now, the biggest challenges from your perspective, the government, the u s government faces on the global scene?

Edward Screven: 05:26 Well, I mean, I think, I think, um, you know, I, yes, I, I think, sorry, sorry. I have a quiet voice. I apologize. Yeah. Alright. So, so listen, so, so, uh, I think, I think the problems that the US government faces actually a very, um, are very similar to, to what our large commercial customers have traditionally faced. Right? Which is, which is that when, you know, when they've thought about, um, solving information problems and they thought about, um, applying, you know, you know, computer technology to, to, to, to, to their particular problem domain. You know, they, they haven't really approached it in a coherent, cohesive way. And so what they've done is they built lots of, um, lots of different, you know, stovepipe systems, you know, with lots of different technologies that, that don't integrate well. And in fact, they spend a lot of money, far more money trying to integrate these systems and run the systems.

Edward Screven: 06:13 And they do. They do actually acquiring them right now. That's, that's exactly the circumstance that our large commercial customers found, um, themselves and a few years ago and are now improving. Now the, the, you know, the, the security angle of that is of course, if I built a lot of heterogeneous systems with lots of different interfaces, with lots of different technologies, and I have a huge numbers of human beings trying to keep it all running, um, it's nearly impossible to make it secure. You just cannot take a traditional it infrastructure and have a high degree of assurance that it is secure. I mean, we build a lot of security technology for products that we deliver to our customers, right? But after we handed over to our customers, what happens? Well, lots of human beings try to make it work with lots of other different components from lots of different vendors. Right? There's a much better way. Okay. The much better way is, is cloud computing. So when we built our cloud where we run enterprise workloads both for government and for private enterprises, we're very, very focused on making sure that we have a fundamentally secure infrastructure that our customers can consume and therefore become fundamentally secure themselves.

Kara Swisher: 07:20 So what he's talking about is the cloud. Everyone knows what cloud your emails in the cloud and everything else. But the idea is that a lot of these systems are moving to cloud systems. The government has been much slower to do this for security reasons and largely because it's largely incompetent when it comes to technology compared to most people, most organizations, um, and that they do on premises work, that that is done by all these integrators all around the beltway, uh, which are used to be called the beltway bandits. And I covered them for the Washington Post. Um, Tucker, why don't you,

Tucker Bailey: 07:50 yeah. So I agree with Edward's point on the security architectures. One of the most acute challenges that we're seeing is actually around talent. Um, you know, as you think about digital talent and the town that's required to compete and succeed in this space, the dod is now competing with Silicon Valley. And when you look at the population of the skills that are required, I've seen estimates that the number of the 10 x servers, which posts from silicon valley, we're familiar with that, right? Those coders and technologists that are 10 x more productive than, than the mean. You have the average of those are, you know, in the low thousands. And then when you further winter that down to the number that can get a security clearance, that are willing to take, uh, a government paycheck, uh, that are willing to go through the turnstiles. And I have access to a lot of the tools that they typically have.

Tucker Bailey: 08:33 You get to a very small population. So how do you compete for that talent? It's very challenging. Um, then there's the point of how do you actually, if you're competing for that talent and that's a challenge. How do you also grow talent? And this is where the Department of Defense in the uniform side is starting to make great progress, especially on cybersecurity. Some of these other, they're creating career fields for these folks, but then you run into retention issues because, right. Would you get to the point where they're competent and talented, they're now in extremely high demand and are being recruited away by the private sector often at three or four times what they're getting paid as a military person. Right. And so then the military and the IC says, well, we can compete on mission. Right? You know, we're going to appeal to their sense of mission and they're going to have a platform to do that here. But if you look at cybersecurity professionals, if they're defending, uh, the national grid or core banking infrastructure, that's also mission-related work. That's national security. So that mission proposition starts to break down a little bit as well. So significant challenge there. I'm happy to talk about it.

Kara Swisher: 09:37 And You yourself, who, who worked for the government, and then now it's in the private sector, correct? That's correct. But yeah, not now giving back. That's okay. Whenever you say it's so, so in that area of talent, I mean, you can't underscore how, how much these technology companies need the talent, uh, the main ones being oracle, Microsoft, Amazon, Google, Facebook, and others that can have all these challenges that the government faces and, and can pay enormous amounts of money as their stock prices increases and things like that. Um, can you just for a second also talk about the idea of training and the problems of our education system compared to, uh, China, uh, in India and even France these days, which is putting enormous amounts of money into the training of more and more people to be able to do these [inaudible]

Tucker Bailey: 10:24 that's a great point. It's another challenge and we looked at secondary and postsecondary education, particularly for digital talent. And one of the things that we found is a lot of universities are building digital programs, AI programs, cyber programs, but under a traditional bachelor's or master's to remodel. And what employers and what the dod and the IC is saying is, I don't care if they have a bachelor's degree or a master's degree, I care that they have these competencies and they can be a philosophy major or they can have a GED. I don't care. Produce that kind of talent. And what they're saying is there's a bid ask spread between the kind of talent that they need and what the academic system is producing. And then if you look in the Washington DC area where a lot of this talent demand is for the u s government, the DC metro region, a region produces three x more digital talent than any other metropolitan standard area.

Tucker Bailey: 11:15 The problem is, is that that's only a third of the demand for that talent in the DC region. And most of that talent is getting recruited out of DC and going to places like Silicon Valley, going to Austin where there's a slightly more vibrant, um, innovation community. Uh, there are startups so they can go from, I'm going to go to a startup, I'm going to go work at a large company. I might go to academia for a little bit and bounce around all in the same area. And DC, you know, is challenged in that way. But there are some really interesting programs where local employers, including u s government and the IC is actually partnering with local universities, great certification programs to say, hey, if you produce graduates with these skills,

Tucker Bailey: 11:54 I don't care what their degree is, I will guarantee you that I will interview a certain number and you know, I will hire anyone that meets our hiring criteria. So there's some good innovation happening

Kara Swisher: 12:01 and it's also hindered by what is largely a homogeneous group of people going into the sector, which is the saying young white men essentially versus all kinds of other, uh, populations that seem to be opting out of that. Um, and most, even the main tech companies suffer from this with persistent, uh, data that they put out every year that shows the same stubborn patterns of, of, uh, of workplace, um, makeup essentially. All right.

Michael Brown: 12:31 If I could just offer on the talent point a, I think that's one of the reasons why Ash Carter set up the defense innovation unit. Because this is a way,

Kara Swisher: 12:38 can you explain that what it was?

Michael Brown: 12:39 Sure. The defense innovation unit, which he set up in 2015 was recognizing that a lot more innovation is happening, especially in certain, uh, sectors, what we call dual use meets commercial use plus military use, AI being examples, cyber, a commercial space, which we're gonna hear a little bit about, uh, later. Um, autonomy. These are areas where there's a tremendous amount of investment relative to what the military is spending an eye, including that the defense industrial base, they're traditional players. So in fact, in 1961 third of global r and D was tied to the u s military. Incredible. That number did 83.7%. So it just shows how much is happening outside and if we want leading a technology, if we want the military to have access to that, we've got to reach out and bring that technology into the military. So again, as it relates to talent, one way to have the folks who are out in those innovation hubs contribute since it's so difficult to hire if you're the government, is to take advantage of what they're doing in the private sector and bring that work in, which is something defense innovation unit does. We also have a program hacking for defense. I don't know how many you've ever heard of it. Real problems with the military has taken to the universities. So let's get professors, uh, veterans and folks who've never been exposed to national security problems all in the same room trying to solve these things. And hopefully some of those folks will be interested in the work that the national security community does.

Kara Swisher: 14:06 So with all the challenge that you find, the most important one that you're facing is, it's not so much that there isn't innovation happening is it's not happening directed by the government, you know, and the government's best probably best technological feat besides the moon landing, which of course we're celebrating now, um, would be the internet, which would, which it created. But talk about what you think the, the, the most challenging, most challenging part of that is?

Michael Brown: 14:31 Well, the most challenging part is, uh, how do we take advantage of all that technology that makes our economy, uh, run so well and have an easier way for the defense department to be a customer. So now we have the challenge as the Defense Department, uh, to say, how can we look like we're an easy customer to do business with? So you can imagine that's an aspirational goal that we have. We have authorities and process to allow us to go faster. And what we're trying to do is work at commercial speed on commercial terms. A, not start with a big requirements document, but just a problem statement that comes from somewhere in the military. I need this.

Kara Swisher: 15:06 Good. Give me an example for reason.

Michael Brown: 15:08 So a good example would be, um, uh, how can we save maintenance costs on aircraft? Think of all the aircraft the military has. And so we went to one of the vendors of, uh, commercial airlines, in fact the vendor that supplies southwest and Delta Airlines and said, how about thinking about, uh, working with the military? This was already a successful commercial company that, uh, really had no interest at the time. We went to them and working with the military, but the ideal kind of vendor for us to be working with because they've got a successful commercial business to build on other people's money. Investors had invested in that platform and that company will continue to innovate on that platform. This is the ideal kind of vendor for the Defense Department where we're not as a taxpayers funding all of that development. And then the maintenance of that, which as you probably know, is a big part of the military budget and the air force, it's, uh, you know, 60, 70% of the costs is maintaining the fleet.

Michael Brown: 16:02 So in this case we said, how about prototyping with, uh, one of the aircraft, uh, in the u s air force, uh, a small a volume aircraft that [inaudible] we showed we could save 28 to 32% of unscheduled maintenance costs using AI and a platform and ingesting data. In this case it was just simple logs, handwritten data, and now we're pioneering that across, uh, different aircraft, not only in the, uh, air force, but also navy and Marines. So this is the kind of idea that we want to work on. It has transformative capability across, uh, the military. So not just working on one niche kind of problem and create a big benefits in terms of costs and readiness.

Kara Swisher: 16:43 It's already being done and innovated elsewhere and paid for by that. Right? That's right. Paid for by the private sector. Um, Edwin, talk about the technologies that you think are critical for the [inaudible] for government officials, not just the defense department, but because security is now everywhere, like including election, including all kinds of things. And obviously Microsoft is showing off this, uh, election protection kind of stuff. What talk a little bit about what you think the key technologies that maybe we aren't paying as much attention to that are critical for the government to be part of?

Edward Screven: 17:15 Well, I mean, I'll tell you what, what, what, what we focus on what we think is most important for our customers, whether government or, or otherwise. And, and, and, you know, we, one thing that's unique about oracle is that, um, you know, we, we have a really wide range of technology from, from the very bottom, you know, like CPU and storage all the way up to, to, you know, very sophisticated, um, applications, right? And so, because of that, um, you know, it lets us focus on, um, defense and depth when we, when we engineer products together, right? So instead of having to think about, um, you know, how are we going to build, build a secure, secure solution that involves, you know, multiple vendor products. I mean, we can create a complete secure stack. Um, now that, that, that fundamentally rest though on, on that secure infrastructure level.

Edward Screven: 18:01 So when we built our cloud, um, you know, one of the things that we did is we realized that that, um, you know, we just can't predict all the kinds of vulnerabilities that are gonna pop up in the world. Right? And you see, you saw this with, with Intel processors, um, you know, over the last few years, right? So like, I mean, flaws that no one could possibly imagined, you know, existing in Intel processors that that would allow, um, data to leak, you know, from one, uh, from one customer to another if they happen to be running software on the same computer. So fortunately for us, when we built our cloud, the way we did is we actually took all of the security processing for the infrastructure level and we pulled it out, pulled it out of the computer that's running the customers code. So we actually, when you, when you use our cloud, there's actually two computers involved, right?

Edward Screven: 18:48 You know, there's, there's a security processor computer and there's the application computer. And so because of that, um, you know, no matter what code your code, a bad actors code, you know, happens to be running in that application computer, it cannot break out of the, of the enclave, you know, the, that that exists for that one particular customer. Okay. And that's just kind of example of, of, of when you moved to cloud, you know, just having a different way of thinking about the problem that that's not a kind of solution that, um, any customer could have built for themselves. It's, it's not, it's not even a solution we could have built ourselves to deliver to a customer, but it is something that we were able to build in our cloud. And, you know, going along with that of course I think is, is we've done a lot of work in terms of artificial intelligence and machine learning to observe patterns of behavior that we see within our networks in order to help us detect, um, you know, detect incidents that we should investigate.

Edward Screven: 19:48 Right? And so at the very lowest levels of our, of our, of our infrastructure, you know, we're scanning, um, all the packets that are flowing through our network looking for patterns, you know, that, that indicate not necessarily, um, match some bad behavior because that's not enough, you know, because new kinds of bad behavior pop up all the time, right. What matters is looking for patterns of behavior that are different. Okay. So when we see some variance from what what we expect, well, that's something we should look at. That's something we should investigate. Sometimes it's perfectly, uh, in fact, most of the time, almost all the time, it's perfectly fine. You know, it's just some different, some different kind of application. Sometimes it's something which actually shows some customers actually been breached through, through the software they've connected to the Internet.

Kara Swisher: 20:30 We're just watching what comes over the five minutes. You see this in the commercial space with Facebook trying to identify yes. All bad actors, essentially what's happening across. Yeah. Which, you know, so, so I think, I think you know, that it's, it's, and that's, that's why I, that's why I'm actually, I'm actually, uh, I'm actually, uh, a cybersecurity optimist. You

Edward Screven: 20:48 know, it's very easy to think, um, hey, the world is ending one, yes, t he v the, the world is ending because, um, uh, because, uh, you know, there are state actors out there and there are right. Who are very aggressive, very talented and incredibly well funded. Right. Uh, and, and, and their interests are not a commercial. And so therefore, you know, they don't take advantage of the philosophy find right away. And so they could be there for years just waiting. Right. So, so, but the reason why I'm an optimist is, is it in fact, I think, I think, you know, the kinds of things that we're building an oracle in our cloud and just cloud computing in general is actually, it's actually, um, changing the asymmetry that used to exist. I mean, in the old days, two years ago, three years ago, okay. Uh, you know, uh, let's see what, what you, what, what you, what you had is, is, is vast numbers of, of of it installations around the world managed by large numbers of people.

Edward Screven: 21:44 Okay. Do have to do everything right every day, not to be vulnerable. So of course they are vulnerable, right? And so, and then you have, then you have a cadre of attackers out there looking all the time looking for vulnerabilities all the time, right? And there, and it just, it just, it just managed. You have, you have one attacker, right? Thousands of potential potential targets. Okay. All of those thousands of potential targets have to invest large amounts of money to try to be secure, okay? That's just grossly inefficient. They could never spend enough money and accurate to be secure in aggregate. But if you concentrate, right, if you use oracle cloud or, or other technologies like that, right? Okay, well now there's many fewer places that we have to defend and we can afford to spend a lot of money securing that infrastructure because it's used by, by thousands and thousands of [inaudible].

Kara Swisher: 22:33 Vulnerability is if there's one now place. So that if it does get attack, that's okay.

Edward Screven: 22:37 Well, I think, yeah, you know, I've, I've heard that, that sort of argument before, I, I don't, I don't really buy it. Right. And, and, and the reason why is that is that, um, if you look at a cloud infrastructure, uh, you know, you can't possibly build it and run it unless it's, it's, it's homogeneous. Okay. I mean, you couldn't afford to do it. Right? And so, and so because our cloud infrastructure is homogeneous, right? We can watch it very, very closely and we can apply technologies to it that we could never dream of applying, you know, in a more traditional it setup.

Kara Swisher: 23:10 So one of the parts that that gives advantages though to those who are, have more malevolent or state attacks on anyone is the idea that, uh, that these, that they do their work is within the military. Like in the Chinese military, that's a path for upward mobility in China. Same thing with Russia. Same, you know, it's very closely tied to the government. Your, you're in the ways that it isn't here. Um, talk about what we need to do to combat that. Because I think our only thing is to be competitive. Have Competitiveness, right? We'll talk about the, what we need to do to, to improve that. We're not going to have a cadre of people in the military that are going to stay there. We're just not. It's just not going to happen though.

Tucker Bailey: 23:51 All right. It's a great point. And so there's a couple of approaches. One is fundamentally rethinking the talent model. So instead of a 20 year civil service or military system where you in your 20, you get a retirement, everything's right. That's just not the way the workforce is working today. And Silicon Valley and other places have adapted to that. The U s government has not by and large, because we have these traditional career paths. So a couple things that I've seen the government doing to be successful there is for certain skill fields. And cyber is one of those. They finally rethought a couple of the models. So there's one model where we're going to bring in young cyber warriors and the value proposition is we're going to train them. They're going to have a three to four year commitment and then the expectation is that they're actually going to go out into industry, into [inaudible]

Kara Swisher: 24:34 so that they can learn the new stuff. Cause what happens is people that are in government don't know the latest or haven't been working cyber wars that come in, they have really, really cool pocket protectors. Those people now I've never cyber boards but okay. Um, yeah so they would, um, they would come in for a short time, which a lot of people are trying, they've been trying to do this with some mixed results.

Tucker Bailey: 24:55 Correct. And so the, the next horizon is how do we think about an in, out, in model where, you know, maybe we train them, maybe they got to private industry, sharpen their skills out there, get exposed to that. And then do we have the mechanisms to bring them back in. And right now that almost takes an act of Congress to bring somebody back in, find a job description and go through the clearance process. But how do you reduce some of that friction so that folks can, you know, job hop to some degree, which is, you know, something that you see quite a bit for this talent.

Kara Swisher: 25:24 What would be a good example of that? Cause they say they're in a military service over there in a government service and then they go out to, you know, silicon valley, which is, which I always call assisted living for millennials because they get everything. They want a dry cleaning, free Kombucha stands, true massage, but not the Jeffrey Epstein kind and then others. So I come on, all right. Anyway, they just get a lot, they get a lot of perks including money and everything else. It's a very comfortable place. How do you then create that besides appealing to patriotism, which I think is what they have been doing,

Tucker Bailey: 25:57 right? So there's a couple of ways. One is, can we actually start with a longer term arrangement, either with the individual or with those companies, you know, so for example, take a Google, right? You'll come to dod, you're going to serve for four or five years and then we're going to guarantee a certain spot, you know, at a certain level, you know, with a company, with the expectation that someday you'll come back, maybe it's requirement, maybe it's not right cause you want to create that dynamic marketplace and you want to keep your own value proposition sharp. But also as you think about what are the skills that we need to build, which may not be in our cyber one oh one for example, training pipeline. So let's say you come to the military for four years, you're an authentic of cyber operator. You then go out to a utilities company and you're working on the defensive side. You're now learning SCADA systems, industrial. You're learning the vulnerabilities there. And then bringing that back into the government as I think about holistic kind of national defense for cyber and then also on the offensive side because they've been now exposed to those specific capabilities. Um, you know, which are in demand

Kara Swisher: 26:59 and these companies are, are, are fighting nation states. I mean you really are. I mean, which is one of the problems is that they aren't getting as much out there. They're doing the work the government used to do.

Tucker Bailey: 27:09 And Kara, this is a huge challenge because if you're a big bank, right, you're seeing losses every day from cyber, right? The fraudsters are very sophisticated using the cyber domain to commit fraud, steal money, et cetera. So the business case is there for them to make the investment because they're countering day to day losses. If you look at utilities players, big infrastructure providers, they aren't seeing the day to day losses because their adversaries aren't the fraudsters. They're the nation states. You have that persistent presence can come in and sit and wait, but because they don't have the day to day losses, oftentimes the business case breaks down when it gets to the CFO. And then there's a bit of a perverse incentive, which is if we have a bad day, it's a national security issue and the u s government will come in and help us. Right. And I think the reality is the government is just not equipped and resourced to do that at that scale.

Kara Swisher: 27:57 But you kind of saw on Facebook they were, they kind of got into that bill and it got too late before they understood what was happening there or, or maybe they did. We'll see. We'll see.

Tucker Bailey: 28:05 And that's a fairly minor example, right? If you think, yeah, we've been talking about great power conflict. If you actually think about great power conflict and activities in the cyber domain, we'll be at scale commensurate with what's happening in the kinetic realm. Right? Can we scale rapidly enough not just to defend dod networks, but critical national infrastructure

Kara Swisher: 28:23 including electrical grids, things like that. Do you think about that? The other things, cause it's defense is now more than, you know, in this recent, uh, back and forth with China, for example, in Russia, what we're disrupting their networks, they're disrupting ours. Is that part of the purview now of these workers that work for you or the idea of what we need to defend from, that's always been the idea that you can send an electromagnetic whatever.

Michael Brown: 28:50 Well, it and the defense innovation unit, we're focused more on what urgent warfighter needs can we solve with commercial solution. So we're not working at the national level in the competition. But of course we do spend time thinking about that. And I would just offer that, uh, what China is doing. And in my mind, it's the most strategic threat of our generation. We can talk about declining powers and other dangerous places in the world like Iran. But if you look over the long term, the next few decades, China is the relationship that we have to understand and, and get right. And we're in my mind not doing the, the amount we should do to prepare for that. So none of us alive have ever lived through a time when there's going to be another economy that's bigger than ours. And I happen to have the view that a national security follows economic and prosperity and technology is the new battleground that allows economic prosperity.

Michael Brown: 29:47 So what do we need to do to prepare for that? So it's things like stem education, uh, federal funding of R and, D, which in my mind produced a lot of the success we're seeing in the economy today. It's the, where Silicon Valley started was a government investment, uh, during the space race. Uh, so we need to think about what do we need to do to prepare for that, to make sure that we're making the investment fundamentally in science and technology, supporting technology and innovation in the economy to make sure that we're as prosperous and competitive as possible in a world where we won't be the largest economy. Um, according to most, uh, most forecasters today.

Kara Swisher: 30:23 Well, we had some questions in a minute, but I want to finish up by something. I was at an event last night with David Sanger from New York Times and, uh, um, and they were talking about the, the concept of a sovereign clouds that there might, that this, the Internet [inaudible], which is this open, chaotic, crazy zone, which has been great for everybody. Um, pre did all these billionaires created all this wealth innovation. Everyone's got a cell phone and everything else. You can do apps, whatever you want to do. Um, the, they may have to go back to that concept. I don't know if you th the idea of sovereign clouds at that there's a Berlin, I think Steve David was using the idea of a Berlin Wall. Now we have to build, or that we have two internets, one authoritarian Internet, which is led by China, which is spreading out all over the globe or ae and the western Internet, which has been the one that's been dominated. I'd love to get a thought up there. That's the idea. And not just sovereign internets for countries or areas, but even companies. There's the Amazon sovereign cloud, there's the Google's offering cloud or the oracle. How do you look at that?

Edward Screven: 31:25 Well, I think, first of all, um, uh, I mean, there already is a starving cloud in China, right? I mean, it, it's just, it exists, right? I mean, so, uh, but I, I don't think, um, I don't think that, that, that, you know, what we should do in the West is say, okay, there's going to be a west cloud that we're going to hive ourselves off from these other parties like Russia and China, whatever. And because we think there's a security threat, right? Because, uh, it wouldn't work. Right. I mean, you know, there, there, it's just like, it's just like, okay, you can't have billions of computers in the west, you know, connected to the Internet. Right. And somehow expect that you're going to be able to make sure that, that, that, that, that, you know, that that state, you know, actors outside the West can't get in.

Edward Screven: 32:10 Of course they would get in, they would be in from day one. Right. I mean, it just, it just doesn't make any technical sense, you know, as, I don't think it makes any economic sense. Right. I mean, I 100% agree. Like economic growth is the key to security. Right. Okay. So [inaudible] so what is the biggest engine of economic growth in the West? It's definitely the Internet [inaudible] technology and so, and so trying to like say, okay, what we're gonna do is we're going to shackle the internet, you know, so that, so that we're going to make it more secure. We could actually just turn it off. You'd be 100% secure if we just turn it off.

Kara Swisher: 32:41 Great for a day. Right,

Edward Screven: 32:42 right. But that, but that, but that, but it's just a bad idea, right? I think, I think, I think what we really need to do is, is invest in technologies that lead led an open internet be be secure.

Kara Swisher: 32:52 Yeah. Maybe we'll just shut off Twitter, but go ahead. Go ahead. Sorry.

Michael Brown: 32:55 I just want to add how old, when should I agree with what Edward Said? It's one thing for China to have walled themselves off with a Great Wall. Great. We need to make sure that we collaborate even more closely with the rest of the world to be our allies, to make sure that we're all collaborating with open, uh, intellectual property, uh, backed by law, uh, talent flow, capital flow. That's the way we're going to be stronger and have an impact on China's behavior. We put $80 trillion of GDP to work against the 12 million that they've walled off.

Kara Swisher: 33:29 Yeah. And then, uh, finally, before we get to questions, what's the one thing you think needs to be done over the next five years that's critical in each of your areas? Whatever, whatever the area. Uh, why don't we start with you Tucker and then,

Tucker Bailey: 33:42 yeah, so my perspective is actually a harnessing some of the technology that's already out there, be it robotic process automation, machine learning, AI. I think the dod is making very good early strides there. [inaudible] but the concept that you can sprinkle AI on existing processes is really tough and it requires a lot of unsexy work. Like going through and thinking about the data rights in every contract that you write. So you get the training data and that kind of stuff and then creating the infrastructure to where you can actually build those capabilities, put them into production in ways that actually scale and are sustainable.

Kara Swisher: 34:11 Yeah, I mean would you, would you agree? I think right now I don't think people realize that technology is coming are so much bigger than everything else that's come before.

Tucker Bailey: 34:21 That's right. And there's your, we've done research that suggests up to 40% of traditional vocations are going to be fundamentally disrupted by this technology. Some will be replaced outride some you're going to have to come to a new human machine interface where the humans are doing the high cognitive function. Machines are doing the repetition, but it's going to require a massive re-skilling of that talent as you're thinking about this.

Kara Swisher: 34:41 And I always say everything that can be digitized will be digital. Everything, everything, but go ahead.

Edward Screven: 34:46 Yeah, I think, uh, you know, I think it's really, uh, for governments and, and commercial enterprises, it's, it's, you know, execute, you know, the plan to move down this road of cloud computing, you know, you know, efficiently and effectively because, because I think fundamentally that is, that's how we get, we get more secure. That's how we, that's how we, you know, flip the asymmetry that currently exists between, between attackers and defenders

Edward Screven: 35:12 and for the Defense Innovation Unit building on cloud. There's many other commercial technology. So I'd like to see them, uh, in very widespread use within the military rather than always relying on something that we designed ourselves and then broader for the society. We've got to commit to a fundamental investment, a generational investment in science technology. For our own economic, uh, superiority and, and, uh, competitiveness for the future.

Kara Swisher: 35:36 And where are we on that?

Michael Brown: 35:38 We're declining. Uh, we have, we basically have seen a decline in federal funding as a percentage of R and, d. It was 2% of GDP in the 1960s and now it's at 0.7 and declining. And I think, as we said before, uh, we're still living off a lot of that press, bury the Internet, gps, miniaturized electronics on and on. We need to make that investment for the next 50 years. That's what China is doing today.

Kara Swisher: 36:04 Yeah. And also if people don't realize it, not just in the government sector, but the private sector and think it's the lowest startup rate in his, in 35 years right now. Is that right? Yeah, that's small businesses. And at the same time, uh, not just that with these large companies, there's not as much innovation of startup of generalized startups. So the last time we had a search engine was never, uh, since Google. And the last time we had a social network, for example, this is just commercial space was 2011, which was snapchat. Um, and there, from what I can tell there that chief product officers and Facebook at this point, so it's a really problematic situation to not keep innovation going. Um, and the only way for innovation to keep going is through competition. And that's how we do beat these authoritarian regimes by being competitive and having small startups bubble up upwards, um, to create all kinds of cool things that are coming. Um, I'm sorry, one more quick question. What's, what would be the coolest thing that you think that they can technological invent? We just showed a jet pack off code for example, which was really disturbing. But what would you think of? What do you think? Like the hovercraft that Larry Page is making or what?

Edward Screven: 37:11 I don't know how cool those things are. Okay. I mean, I saw the one flying over my house, that's for sure. Yeah, I mean, look, I think, I think, um, I think, um, you know, uh, I think there's a lot of room to go in terms of, in terms of applying machine learning to all kinds of interesting problems, right? I mean, you know, there's, there's, there's the kinds of problems we see in front of us every day. Uh, like image recognition, you know, those kind of things. Okay. Um, but, but like what we're doing at Oracle is we apply AI and machine learning to business problems. Right. And I think, I think, you know, using machine learning to, to make, to make, you know, accurate data, different driven decisions I think is, is it's kind of under the surface. I don't think a lot of people think about that, but, but I think it has the potential to have a really fundamental impact

Kara Swisher: 37:54 patterns and things like that. Anything else? Exoskeletons?

Michael Brown: 37:58 So you'd have to say in terms of broad applicability, military plus the commercial AI and the combination of a g five g

Kara Swisher: 38:07 no one, none of you mentioned Elon Musk's neural net link that out people's heads. I did an interview with him where he said that AI is not going to kill us, but they're going to treat us like how, how's cats? Yeah. And that we need to put a chip in our head. He said this several years ago so that we can keep up, um, or they're gonna it's gonna just run us over the way. You would run over a, uh, a group of ants when you're building a highway, which was such a nice view of the world. Anyway, questions from the audience? Let's start right here. You Sir? Yes. Oh, okay. Wait for the Mike. Sorry. All right. Sounds like you have a deep voice though.

Audience Member: 38:43

Thank you for that. Um, every day we see read about and impacted by a lack of a better word, break-ins. Uh, they steal our social security number. Every credit card company has been, uh, challenged. You get all kinds of emails about how we're gonna protect you for the next year because all your information went out. Um, it's really getting old. Um, and I have a sense it's not going to get any better, but I'm hopeful that you guys can tell us we're on the right trajectory and we're gonna stop all this stuff so I don't have to get IRS codes to put on my tax return and change all my credit cards three times a month. Where the hell are we going with this? Right? I'll say I'll start and love to get other's opinions. I think the good news is that's actually getting better for your own personal security and privacy.

Tucker Bailey: 39:40

Right? In some ways it's the new normal and you know, it's something that we've just adjusted to and our adjusting to. Uh, but also it's about detection response. How quickly can we detect that before they've actually kind of used your social or something like that. But the biggest change that I see coming that's happening now is the move away from username and password, which is incredibly insecure, right? It's not that hard to get somebody's password, but as you go to biometric identification, token based systems, it makes it that much harder for someone to get access to your information.

Kara Swisher: 40:09

Yeah, that's so comforting. They're going to have your eyeball. In other words, I say no, I think it's going to get worse. And by the way, it's not necessarily hacking. One of the things that I always say to people is what happened with Facebook, for example, which got a lot of media attention, stuff like that. The Russians were customers of Facebook, they didn't hack it. They were customers.

Tucker Bailey: 40:26

Well I think the economy is gonna get worse and better because some things are improving as Tucker just talked about. But then the degree to which technology is, uh, expanding sensors by g, the attack surface just got a lot bigger. So some things improved, but now there's a whole, Michael Brown: 40:45 yeah, let me just give you some sort of good, all those kinds of attacks that you mentioned, all those kinds of breaches. Right. Um, you know, we study those, right? Okay. Cause we want, we want to understand many of them are our customers, right? Because we understand when I understand what happened, right. And most of the time, most of in most of those breaches, the, the fundamental problem was human error. Yes. Okay. It was people did not correctly configure the systems to be secure. Um, and most commonly, um, people did not apply patches to the software to actually make it secure. I mean, software has bugs. Some of those bugs are security related. You know, we, Oracle and other vendors, you know, we produce patches. Our customers often don't apply them. Yeah, okay. Um, sometimes very often our customers can't find all systems running all the software that needs to be patched.

Michael Brown: 41:36 Right. And, um, and so that's that, you know, it's, it's that, it's that morass okay. Which, which has created so much consumer exposure to, to vulnerabilities. Yeah. Right. And that is why actually I'm optimistic, right? It's because we're moving too to a time when, when there's much less, uh, infrastructure in the hands of, of these companies that are holding your data, they rely on a much smaller number of parties to deliver the infrastructure and do the patching. Just just to give you an example, I'm going to have to get the other question, but go ahead. Okay. Just to give an example here. So, so, so when we patch our infrastructure, we patch millions of servers and less than 24 hours. Okay. It's completely automated. Our customers, by the way, don't even know we patched, right? Because we've developed technology that allows us to apply patches without taking software down. Okay. So that's that. That's why it's getting better right now. Basically we have to get rid of humans. Okay. Next let, let's actually, let me get, um, let me get, uh, go ahead. Go ahead. Right there. Right here.

Audience Member: 42:42 Thank you. I'm just wondering, this being next year being an election year and a census year. Yeah. How reliable do you think our voting machines are in terms of counting the votes?

Kara Swisher: 42:53 Well, that's next. The next, he's going to talk about that on there next. Yeah. Yeah. Not Very. Um, so just overall it's a disaster. That's my question. Particularly v Visa Vi what the rest of the world does. Yeah. I know it's a state by state issue, but I'm curious to your views. Yeah. Your votes probably not counted. But go ahead. Next over here, over here, over here. And then real quick, but like I am, I'm sorry. That's my famous role in Silicon Valley. It keeps them honest.

Audience Member: 43:23 Yeah. I'm Guy Swan from the association and the U S Army and a member of the Homeland Security Experts Group, uh, for Mr. Brown. Uh, question for you, uh, with so much outreach now from the Defense Department to industry, how do we deal with things like the recent Google employee backlash on some, uh, Defense Department programs? Uh, that's my first question then slightly different off the cyber just a bit is, is additive, uh, manufacturing in three d printing the panacea. We hope it's going to be

Kara Swisher: 44:00 three d printing [inaudible]. Okay. Gotcha.

Michael Brown: 44:02 First on Google and, uh, Maven, uh, and defense innovation unit was involved in helping as the defense department put together, uh, vendors for project maven. Uh, the good news is I think this was incredibly well covered by the media and as it would, uh, reflect, uh, broad views in silicon valley overblown. Um, so there's different kinds of vendors that we work with. Uh, most of them are small companies. They're delighted to have an opportunity to work with a customer as large as dod. Today when we ask for help on a problem, we're working, we get 30, 40, 50 submissions for each problem. So plenty of help. It becomes more complex for these large multinationals. Google being one. I think they've learned they wouldn't in the future want to crowdsource their business strategy. And I was pleased to see some of the other multinationals, uh, Amazon, uh, Microsoft, Amazon loves doing, I mean, yeah, they've come out and said, you know, the place to exercise that is at the ballot box and we need to support the government. So that's, that's great to hear.

Kara Swisher: 45:05 One of the problems with that is that the companies have let their employees talk for years. Now Google had named Jen, they had these meetings where employers get together and scream at the founders almost every week. No, they do. It's like, I don't like the Kombucha this week. And they yell about it. And so they created a, an employee base that feels that they're part of the system and they are

Michael Brown: 45:27 so, so the bottom line on working with the Defense Department is we need to just be an easier customer for those companies. And that's about speed and getting some money to the right customers just quickly on atom manufacturing. I don't think it's a panacea, but, uh, incredible progress made with metals with concrete. Yeah. We're now working on a project to allow forward basis for the marines to be built with additive manufacturing on concrete. So imagine bridges and uh, barracks being built with Eder manufacturing using [inaudible].

Kara Swisher: 45:54 There's some cool commercial companies like carbon and some others that are really cool in that area. It's an area. Okay. Uh, last, last question right here. Sorry. Sorry. You can all grab these guys.

Audience Member: 46:05 Sure. Thank you very much. My name is bishop garrison. Just a quick question. We've talked about all these new evolving technologies. When you talk about machine learning, AI and you talk about the skill sets necessary to deal with them, particularly from the next generation in your respective organizations, have you really, uh, began looking at a training and ethics and the development of these technologies and their deployment?

Kara Swisher: 46:26 Yeah, that's an interesting topic. That wet blanket here, writes about that in the New York Times a lot. They also need to take humanities courses. Talk about that and then we'll finish.

Michael Brown: 46:35 Yeah. So, so just I can tell you at Oracle, I mean, I mean we have a large, um, AI machine learning research group and we have, you know, machine learning, AI experts kind of spread throughout our engineering organization. And so, you know, by bias and, and ethics is definitely something that we, we take into account just as a, as a matter of course. I mean, we don't, we're very careful to try to make sure that we don't wind up in coding. Um, you know, human bias, you know, into the, into the models. I mean, if you think about it, it's, it's not just the right thing to do. It's also the most efficient thing to do. Right. You know, with, if we're trying to, right, if we're trying to find the best employee to do a job, if we encode human bias, that probably means you're bypassing, you know, one of the better candidates. So we don't want to do that. Yeah.

Kara Swisher: 47:15 And it's anything and any others than that,

Michael Brown: 47:17 the Defense Department, uh, as we have to do with all technologies is looking at what are the, uh, uh, implications ethically. And the joint AI Center recently set up at the Pentagon is, is working on this, uh, very actively

Kara Swisher: 47:28 and going to be a big issue in facial

Speaker 1: 47:30 recognition right now. Obviously the company that makes the cameras that are on police departments doesn't think facial recognition is a, is it should be used yet cause it's so bad. I might point you to an interview I did with Andy Jassy who head of AWS at Amazon, which is an a massive business. They're a around their recognition software, which has been controversial, but it's an interesting debate on the issue. Anyway, this is great. Thank you so much. And I'm sure there'll be tons of [inaudible]. I'm already talking about next year. Thank you. [inaudible].