Steve Clemons: OK. Now we're going to talk about the world—you're going to be my Dr. Strangelove, OK? On all the bad things. But before we get there, let me start with you, Samir. One of the questions, as you sort of look at cyber defense or cyber offense as well, is what kind of norms are evolving in the international system that you think matter? I mean, you did this for Barack Obama and Susan Rice. You were out there trying to do smart policy in cyber. So I'm interested in what some of the features of those norms are, and whether or not you feel that we're succeeding in evolving towards them.

Samir Jain: I think it's a mixed picture. I think we've made some progress at the UN and in sort of multilateral and bilateral relationships, where there has been some consensus on norms around not attacking critical infrastructure.

Steve Clemons: Do you believe that? Do you believe that the states that are participating are not attacking each other's critical infrastructure?

Samir Jain: You have to differentiate between state actors—sort of cutouts, people who are sort of affiliated with states—versus cyber criminals. I think there's a lot of what I would call preparation, so that people are positioning—the nation-states are positioning themselves, so that in the event of a conflict or something like that, they would be in position. So they may be positioning malware.

Steve Clemons: So that's a mutually assured destruction thing?

Samir Jain: Almost, almost. Almost like that. But I think even as we've made some progress, and it has been halting—and you know, the UN group of government experts this year wasn't able to agree on additional norms—I think the flip side of that, and where we're having a lot of trouble, is figuring out, even if we get agreement on some norms, how do we enforce them? In other words, what's the punishment or the consequence if you don't in fact obey that norm? And I don't think we've figured that out yet.

Steve Clemons: When did you leave the White House?

Samir Jain: January.
we find most continuity, mostly because as far as you can see, for the time being at least, the work of the current administration is very much a continuation of the work of the previous administration. So from our perspective, from that point of view, we don’t see any major problem. The only diplomatic—and I shouldn’t say it—but perhaps concern that we have is that right now it’s slightly difficult to find the counterparts in the administration, that we talk to.

Steve Clemons: Yeah, I was going to say, who do you deal with? Like who’s your interlocutor?

Andrea Glorioso: Well, at the State Department, just recently, there was the appointment of the assistant secretary for—there was a merge of the previous digital economy and cyber position in the State Department. So we now have that interlocutor whom I met. He’s great. We now have a new at least appointed secretary for homeland security. So we kind of have the counterparts, but certainly I think we are still waiting for the full picture to form the administration.
cybersecurity. And if you look at that executive order, which for the time being is very much about reviewing the internal preparedness of the federal government—and also, that’s of course very interesting for us—preparing the international cyber engagement strategy of the U.S. government—if you look at that executive order, what is on paper as opposed to the various drafts that were leaked from January until May, that executive order is very much in continuity, as far as we can tell, with the work of the previous administration.

Steve Clemons:
So Gordon, I’m grossly simplifying what I just heard, but norms are evolving, structures are coming in, warm and fuzzy, sounds good. Dr. Strangelove, do you see the world the same way?

Gordon Goldstein:
Well, while diplomats at the UN are busy continuing a discussion about norms, perhaps not as effectively as they should, and in Europe the conversation continues—while that dialogue diplomatically is going on, the great cyber game is being played, and it’s being played with enormous intensity.

0:06:00
What we now know is that those offensive cyber weapons were stolen from the United States, from the National Security Agency. From our cyber command.

Steve Clemons:
So if the NSA is getting hacked, what chance of survival do we have, right?

Gordon Goldstein:
As one of those movie titles said, “Be afraid. Be very afraid.” If the dominant cyber power in the world, which I believe the United States still is, competing with China and Russia and Iran and North Korea—if the dominant cyber power in the United States cannot safeguard its own offensive cyber weapons, and they end up in the hands of third parties, and then in the hands of rival nation-states, how much progress are we making in alleviating the threats of the global cyber risk environment? I think this is an extraordinarily important kind of epical moment in how the game is played.

0:07:00
Steve Clemons:
I had no idea how dark you could be, but I’m impressed.
[laughter]

Gordon Goldstein: Playing to type.

Steve Clemons:
I think in this area, when we’re looking at the ecosystem, one of the things that has happened recently—I’ve had the privilege of talking to Ambassador Mike Rogers of the NSA, who is dual-hatted, who is head of the National Security Agency and also head of the Cyber Command which is now a full combatant command. We have some folks from there here. He’s talked a lot about in the world of norms,
almost trying to figure out how you get back to a system of deterrence. How you create—it sounds like a more punitive side, but how do you bring back some of the risk/reward dimension or punishment/reward dimension of this? And Samir, I know you’ve thought about this in terms of policy framework. And is it achievable? Because you just mentioned North Korea and Russia—two countries of vastly different resources in this arena. What should be shocking is North Korea—I can’t believe North Korean can penetrate—I mean, how does North Korea do it? It’s the most cut-off nation in the world.

And yet somehow it has extraordinary capacity. What would you do? I mean, how do you fix this?

Samir Jain:
I mean look, I agree that in the foreseeable future, the cyber problem in many respects is going to get worse before it gets better. Because I think the attack surface is growing. The number of actors who are able and willing to engage in cyber attacks is increasing. And frankly, we haven’t seem some of the worst kinds of cyber attacks that we could. So I think we’re very much at the beginning stages.

Steve Clemons: What are those?

Samir Jain: A, we haven’t seen many cyber attacks yet that have physical consequences. We saw the attack on the Ukraine power grid. We’ve seen ransomware that has some effect on hospitals. But we haven’t really seen major attacks—you know, dams being taken over, and the sluice gates being opened and causing flooding downstream, which is very possible. And we haven’t seen attacks that—what I would call attacks on data integrity. So that instead of stealing information or denying access to information through ransomware, someone goes into a financial system and adds a zero to a trading order, or deletes a zero, or goes into a hospital system and changes the dosing information for patients.

And so, you get changes in the integrity of the information, it’s not recognized, and people act on that, and you have an undermining of confidence in the whole system. You know, the financial system.

Steve Clemons: What about the Securities and Exchange Commission hack, and Edgar? You don’t think that somebody may have gone in and shifted information here and there inside Edgar?

Samir Jain: It’s certainly possible. There’s as far as I know no public indication that that happened. But yeah, that would be a possible... but that’s the kind of attack that I’m talking about, in terms of one way in which this is going to get worse before it gets better. And look, I think one of the things that we tried to do, and I think this next administration is continuing, is to recognize that in order to tackle the cyber problem, to increase deterrence, you really have to look at all tools of government. In other words, a cyber attack can’t simply be responded to on a cyber level. You have to look at whether it’s sanctions or other economic measures, diplomacy, law enforcement.

And all of these different tools have to be brought to bear. Are we there yet in terms of achieving deterrence? Clearly not.

Gordon Goldstein:
Can I jump in on this question? You’ve identified the seminal question—how do you reinforce our cybersecurity program, our cybersecurity strategy, with an element of deterrence which has been lacking? And some of our best thinkers in the U.S. foreign policy community are really focusing on this now. Joe Nye, the professor at Harvard who has been one of the leading political scientists of his or any generation, has just written a tremendous article on deterrence and dissuasion in cyberspace, which students in the field, I recommend it to.
Andrea Glorioso:
So first of all, I’m not sure we would like to be called an offshore center of anything.

Andrea Glorioso:
But besides that, so you’re asking for my personal view, and that’s what I’m going to offer you. So this is not official EU position. I think that the way I certainly look at the Americans after more than three years here is that I find you guys a bit naïve, to be completely blunt and honest, in the sense that the kind of hybrid warfare that people are alleging has happened here in the U.S. is something that is very familiar to us in Europe, for decades. It’s not anything new. And independently of who actually is behind those alleged attacks—and by the way, I would also like to point out that when we talk about norms and all this discussion, let’s not forget that attribution is still very difficult.

Steve Clemons:
Andrea, let me ask you to take off your EU hat for a minute.

Andrea Glorioso:
I can’t. [laugh]

[laughter]

Steve Clemons:
Yeah. But I’m interested in having an offshore perspective of us. When you look at what Russia has done with hybrid war in places like Ukraine and elsewhere, what’s happened and whatnot, do you look at the United States as slightly befuddled, uncertain?

0:12:11
How do you look at the American both private sector and public sector response to some of the things happening in the world? And are you worried?

0:13:05
Any country can claim that another country is conducting an attack. That doesn’t mean that that country—and whether that country is the U.S. or Russia or European country, et cetera. Let’s keep that in mind. So there is that. Second, I think that we should all keep in mind that this is not so much an American issue. I think it’s an advanced economies issue. So it’s European and American. The reason why the WannaCry, or one of the reasons why the WannaCry virus Gordon has mentioned was effective is because 99 percent of the systems that were attacked with that particular virus were unpatched for a vulnerability that had been known for years. So, there are geopolitical issues. There are state actors that are moving there. So it is a dangerous environment. But let’s not forget that a lot of what we’re talking about is unfortunately the baseline of very common cyber hygiene that is very low. And this is true in the U.S. as it is in Europe. I would argue, as a European in this wonderful country, you have perhaps slightly even worse problems, because your IT penetration is slightly higher than in Europe.
0:14:07
It depends on the European country, actually, but by and large, you have IT systems penetrating—or the Internet or whatever—penetrating into your infrastructure at an even higher degree than you can find in Europe and other countries. In this way, you’re more vulnerable. But again, let me underline that yes, there are kind of state-level, geopolitical issues. We need to address those. But there are also very basic issues of patching, of basic security, that are not being addressed.

Samir Jain:
And this problem is going to get worse, because with the advent of the Internet of Things, and the spread of connected devices…

Andrea Glorioso: Indeed, yeah.

Samir Jain:
…through homes, factories and the like, many of—in which it’s not clear that the incentives are there to actually integrate security even to the same level that you have in the rest of the infrastructure—I think this problem of basic cyber hygiene is going to get worse.

Steve Clemons:
How is there not the incentives there to embed an Internet of Things environment—when you have companies like Sysco or Accenture or Microsoft and others that provide the capillaries and the system for some of this to work?

0:15:08
I hear this thing about there not being enough incentives. What are the right incentives to get it? I mean I just—it sounds just crazy to me.

Andrea Glorioso:
First and foremost, I would say that because it is a very complex environment, and we should not forget—we should not be too quick to attribute responsibility to companies which are trying—whether they’re American, European, or from elsewhere, they’re trying to do their best, by and large. But the environment is complex. From our perspective—and here I’m putting back the EU hat, because this is an official position/reflection that we are conducting in Europe—but the attributional liability is not at all clear. When something goes wrong, who is liable? And as we are moving towards of an Internet of Things world, in which you have a toaster which is connected to the Internet, to understand when and what time—and by the way, it’s probably connected to my tracker to understand at what time I’m waking up, whether that morning I wanted white bread or black bread, or whatever. If something goes wrong and if that toaster is used, for example, for a distributed denial-of-service attack—and this is not science fiction, this is what happened with the Mirai botnet one year ago, more or less—who is responsible?

0:16:08
Is it the toaster producer? Is it the tracker producer? Is it whomever has been handling the data? Processing of data? Communication of data? Until we manage to come to some clarity on who has liability there—and there are various ways in which you can do it, and we have our own ideas, but they’re not necessarily the right ideas—the problem is that companies will never—rationally speaking, no company will ever invest money into something until they’re told, “If you don’t do that, there is going to be a cost for that.”

Gordon Goldstein:
This is a critical question. And I’m going to play to type for you, because I know you’ll like it. I hosted a meeting at the Council on Foreign Relations last spring. The title of it was, “Will the Internet of Things be a Cybersecurity Disaster?” And the question…

Andrea Glorioso: Yes.

Gordon Goldstein: …is…
[laughter]

Gordon Goldstein: The question is not a facetious question. It’s a real question. There
are a billion additional connected devices every quarter.

0:17:01
Every quarter, a billion additional connected devices are connecting to the Internet. And we have not had this difficult discussion...

Andrea Glorioso: Yeah.

Gordon Goldstein: …about how we're going to achieve a basic modicum of safety and protection in that evolved world.

Samir Jain:
And what's important I think is that as you get all these devices out there, it's not simply that those devices are targets in and of themselves. But they can be weaponized and used essentially as weapons against the rest of the infrastructure, which is what happened with the Mirai botnet. So it sort of has an exponential effect on the problems of security.

Steve Clemons:
Just before I go to the audience, I want to ask you quickly about China. If we were doing this event two years ago, China would dominate the discussion. Now we're talking about a lot of other countries. And Samir, I know you were involved in the Xi Jinping Obama discussion on establishing norms and getting China to back off. Whether it has or not, I think you're in a slightly different—you believe that China has been a good player, good behavior, ought to get a gold star.

0:18:00
Samir Jain: Well, I'm not sure I would go that far. I think it's…

Steve Clemons: You'd go partly there, right?

Samir Jain: Partly there. I think it's true that if you look at…

Steve Clemons: A purple star.

Samir Jain: [laugh] If you look at the amount of cyber-enabled IP theft, which was the main focus of that agreement, that China or Chinese actors have engaged in, that has been reduced. And I think the government has said that, but I think also third party cybersecurity firms, private cybersecurity firms, CrowdStrikes of the world and whatnot, have seen a reduction. Does that mean they've stopped? Absolutely not. Does that mean they couldn't increase—I actually think what they've done is become more strategic. In other words, I think previously what happened is that there was sort of a “Whatever we can hack, we will hack,” whereas now there's a little bit more control and more strategy, and they're more strategic about what it is that they're hacking.

Steve Clemons:
So it's not a good story. Andrea?

Andrea Glorioso: Can I jump in on this? And I didn't know I could do that, but I will take off again my EU hat and offer a personal perspective.

Andrea Glorioso:
It's great. No, I love it too. There are many things I would like to say that I cannot say…

Samir Jain: [laugh]

Andrea Glorioso: …because of the EU hat.

0:19:00
So look, personal observation—I think it's important and very much related to what you asked me before—how do non-Americans see what's happening here in the U.S.? Let's not forget that—and by the way, the European Union and China have deep disagreements on many, many, many issues. I don't think we can be defined as friends, and I want that to be clear. But I think it's important for the U.S. public
Steve Clemons: Thank you. Let’s go to you. Questions? Thoughts? Right here in front. We have a mic? Thank you so much. Give you a round of applause for all the running. Hi.

Person: Oh.

Steve Clemons: It’s Teiko [sp], right?

Teiko McCollough [sp]: Yes, yes. Hi, my name is Teiko McCollough [sp]. My question really is for you, Andrea. Can you speak a little bit to GDPR or the general data privacy regulation that the EU just is actually about to implement, this coming May, and where that lies in the establishment of the cyber frontier between the EU versus the rest of the world?

Steve Clemons: Thank you. And I’m going to ask for short form, so we can get a couple real fast.

Andrea Glorioso: Sure. Very briefly, the GDPR—the General Data Protection Regulation—is the law of the land in the EU since last year if I remember correctly.

0:22:04

Indeed it will become enforceable as of May 2018. I think that what really matters in terms of[0:22:09] European actors is that there’s a provision in the GDPR which—by the way, we believe it was always—from a jurisprudential point of view, was always the case. But now it’s statutorily put in the law, that if you handle— if you do business with Europeans, if you handle data of Europeans, then that European law should apply.

Steve Clemons: Thank you. Other—yes, right in the middle.

Andrea Glorioso: Wow, that was fast. [laughter]

Andrea Glorioso: We can perhaps talk more about this later. [laugh]

Steve Clemons: Right there, yes.
Andrea Glorioso: Wow.

Nicole Carolin: Hi I’m Nicole Carolin. I’m with the Internet Society. And my question is, if you could talk to the people negotiating NAFTA right now, what big opportunity would you insist that they talk to their colleagues about?

Steve Clemons: So NAFTA and the Net.

Gordon Goldstein: I’m going to pass that off.

Steve Clemons: Samir?

Samir Jain: I mean, I’m not a NAFTA expert, but I think the question of trans-border data flows is an important one.

0:23:05
It’s something that could be dealt with in NAFTA. I know it was sort of an issue in the TPP that was eventually—that we were pulled out of. So I think thinking through sort of those kinds of issues, whether it’s done in the context of NAFTA or otherwise, is very important.

Steve Clemons: And last question. I saw another hand. Oh, in the very back.

Andrea Glorioso: And that was NAFTA in 20 seconds. So. [laugh]

Samir Jain: [laugh]

Mark Batenchuk: Hi. Mark Batenchuk from Scope Group. We are the only cybersecurity recruiting company in the D.C. metro area. And so one of the things that I always like to try to do is look around the corner. You all are experts, and as we wrap up this great presentation, can you guys give us a little insight as to what we all might be talking about in a year? What the topics might be one year from now...