GUS – DEFINING A CYBER MOONSHOT
VIDEO TRANSCRIPT

0:00:00 to 0:14:33

0:00:00
[applause]

Person:
All right. So first, thanks, particularly to The Atlantic for great cooperation and us pulling together this event together. This has been absolutely terrific, and we're thrilled to be partnering with you on something I think is just so important for us to talk about. And thank you to Representative Hurd for actually setting a lot of the stage for what I want to cover today in this very quick talk about this concept that we're calling the cyber moonshot across the world. And so before we step in, I wanted to introduce the cyber moonshot concept, and help people understand that this is a call to action. It's about us changing the game in cyber, swinging the pendulum back in our favor, and aggressively attacking the cyber problem to position us on the high ground. It's about establishing leadership and concerted action to accomplish a goal. And it's something that I think we have to do now, and we can't put it off any further.

0:01:01
Our intention is to really stop talking about the problem—although I will talk about the problem a little bit in the next couple pages coming up here—and then to act coherently to address it, right? So it's not that we don't have action. I just think that we don't have sufficient coherent action that allows us to move aggressively forward in a common direction. We want to set a BHAG—you guys know this term? Big hairy

audacious goal, of shifting the balance of cyber power in our favor, and establishing a secure cyber foundation that we can with confidence build a future on. And it's about creating real and demonstrable change to make the nation's data secure, and the nation itself cyber-safe within five years. And that's the cyber moonshot. All right, so as we all know—and you've heard this too often, by any measure, and you just heard several of them up here—things are bad and getting worse in cyberspace, right? And this is true despite an increasing rate of cyber spending across all private sector and government and things like that, the hard work of so many brilliant people that are trying to address the problem and bring solutions to bear, and our astounding investments.

0:02:08
If anybody ever goes to RSA and attends the conference [0:02:10], the amazing investments we have in new technology, new capabilities, that are constantly appearing on the horizon across the board. We know the fact that threat velocity continues to increase. Nation-states no longer hide their hands. I think that's one of the most scary outcomes that has occurred recently across the board. We have breaches that affect hundreds of millions of U.S. citizens and billions of people worldwide across the board, and active meddling in election attempts, and things like that. So all those things have been happening. So what's really interesting to me personally is even my parents—my mom is 88, my dad is 93—they are now asking me and holding conversations on a regular basis asking me about how can I be safe, and what's going on? And they're really worried about the fact

that their personal safety is in jeopardy if they use services in cyberspace, and that their hard-won savings are in jeopardy if they're not careful about these things.

0:03:01
So imagine—so this is a conversation which has elevated to a point that I don't think we've ever had it before, with just basic constituent people across the board. And now, given all those other things, comes this wonderful world of the Internet of Things, where we're going to have a ten- to 100-fold increase in connected devices across the board. And this is a world of boundless opportunity. I mean, if you look at what we'll be able to do through the Internet of Things, it's an astounding thing, right? Better healthcare, more efficient citizen services, fully smart and integrated cities, reduced greenhouse gas emissions, agile and adaptive military forces that enable us to deal with things on a much better basis. It's also the world of cyber nightmares. Security is an afterthought in this mad rush to market around smart devices across the board. In a world where you're only as secure as your weakest link, the fact that you have 100 times as many devices connected means you have 10,000 additional points of attack that can be brought to bear against you, through any mechanisms there.

0:04:00
So the numbers are overwhelming, and we've already seen an instance of this through the Dyn attack—the Mirai botnet that took place a while ago. Anyhow, so this I believe is the biggest crisis looming on the horizon, and it's already running us down. And we can't continue business as usual, because the numbers simply don't scale. We cannot throw people at the problem. The math simply does not work. So fortunately in this case, well, hope is on the horizon—and I'll hit this a little bit—through AI and machine learning. We talked a little bit about this—quantum computing I think might be able to help in some of these areas as well too. But I think we can all agree that solving our cybersecurity challenge and making the nation's data secure, our citizens safe, protecting our critical infrastructure, is maybe the single most important thing that we can drive to achieve today. The world's economies are completely interdependent on this thing called the Internet, and cybersecurity is a problem that thus affects all of us, across the United States, across the globe. It knows no boundaries, and it has no bias. So it's not something [0:04:58 that we're going to do?].

0:05:00
We used to worry about this thing called MAD—mutually shared destruction—many years ago when I was a kid. This is important to what's going to follow up here in the rest of the talk. Now we worry about a new MAD—mutually assured darkness, right? So the ability for people to disrupt our economic foundation of our modern world, damage and destroy our life-essential services and rupture the fabric of our society and our daily lives is not the stuff of science fiction, but it's a very, very real problem. OK. So for the next few minutes, I want to give our thoughts on what it's going to take to land this thing we call the cyber moonshot. So let's roll back in time. When the original moonshot was proposed by President Kennedy, there were three specific things that actually led to its success. One was inspirational leadership. The second one was a specific call to action in order to accomplish a goal that many thought was unattainable at the time. And the third was a commitment from Congress to provide sufficient funding so that they could do sustained investment in order to accomplish the objectives that were set out. And what's most important about this—it was a challenge that ignited the nation to work together. It excited the passion of young minds. I wanted to be an astronaut.

0:06:00
It focused on energies and our intentions and brought government, private industry and academia together in the pursuit of an audacious goal that many thought was unachievable. We need this today in the cyber realm. That kind of purpose, focus, and energy to drive this forward. Even Hollywood and the consumer industry were in on the mission. So

"Star Trek" came out as part of—in the same era as the moonshot was being developed and going on. To boldly go where no man has ever gone before, right? We still use that phrase today. You'll see it a lot, right? But more importantly, we had Tang, OK? The astronaut's drink, right? I drank a lot of Tang as a kid, I have to tell you. And so today, we need to ignite that same passion, that same attention, joint action, and a focus on a much harder and much more important problem to make the nation cyber safe. And I think the citizens of our country deserve nothing less. So I want to emphasize that when we think about this, back in that day, almost all of the basic science and technology was already really understood, and a lot of it was already in place.

0:07:00
We had rockets. We knew about escape velocity. We knew the mass of the moon. We had built space capsules. We had space suits. And yes, we even had Tang, right? Tang proceeded the Apollo program—1958 was actually when Tang was invented. But it took a visionary challenge to bring it all together in order to put it in a way that allowed us to accomplish the goal. We are in the same position today. We actually really well understand the problems that are out there. Right? We have a lot of great technology. We know what it takes to be successful in many, many areas across the board. We have exemplars of success that we can take advantage of. But we lack I believe this coherent focus to make us work well together and to drive to a common, achievable goal. So again, it's not that we're not having action. It's that we lack a coherent focus on action in order to drive us forward and get the job done. So I'm going to focus quickly on five things that I think are really essential for us to really look at to drive ourselves forward as we do these things.

0:08:04
So most important—well, the five things I'll get to. Most important, we have to think about this as a journey. It took eight years to put the man on the moon and bring them home again. So you can't look at this as a one-and-done. It's something that we're going to be on a pathway to achieve for a while. And we'll need a systematic and methodical approach in order to get there. Our goal has to be for how to leap ahead of our adversaries, and we have to bring a different mindset. So we're going to have to apply techniques that our adversaries use against us in order to actually build defenses in a way that make it much harder for them to be able to do the things that they want to be able to do. So beyond basic hygiene, which as Representative Hurd said, is actually critically important to do, it is really—I think there's these—we should be actively moving into five particular areas that I think deserve a lot of focus. First and foremost, along with basic hygiene, which is a passive and a reactive thing but critical to do, we now need to step aggressively into proactive defense.

0:09:03
We have to stop firefighting, and we have to be begin to start fireproofing. We have to apply proven and effective practices—hunting, red teaming, continuous vulnerability scanning—to probe and root out attacks and APTs before they get a chance to do damage and sit in our systems and do things like that. We have to bring to bear machine learning, and AI in particular, to enable detection response [0:09:27] machine speed. And we must do this in order to deal with the IoT challenges facing us as we move on ahead. You have to go through the cloud. I mean this very, very seriously. What's really interesting about the cloud is not what its capabilities are today, but the fact that within the cloud, there are nascent capabilities that we can take advantage of that will enable us to redefine how we approach security, and are critical enablers of getting to cyber resilience. And this is the latent promise of the cloud. We have to go and harden our data. We talked about this a lot. Most of the events we've seen in the past have all been about the fact that we didn't harden our data sufficiently.

0:10:02

And I believe that because we've known how to do this for a long time, there's actually no excuse for [sic] doing it. So tokenization, encryption, microsegmentation, and blockchain, which was mentioned earlier—we now have techniques and capabilities that I believe give us no excuse not to harden data and things like that. We have to do security by design. Security must be built in at the beginning of every action. We ought to move ourselves into a world of DevSecOps and agile methods, and bring together business IT and security at every sprint and every step along the way, so that you can make the most effective use of your dollar spend. And that's what's critical. Because in a limited budget world, how do you make the most effective use of your dollar? And then finally the goal is to build in cyber resilience. Resilience is an ability to take a licking and keep on ticking. And so for those of you old enough to remember, that's the Timex line from the Apollo days. For those of you young enough, I'm sorry—yet another moonshot era reference that you may not recognize. But remember, it's not about cyber perfection. And I think that's probably one of the other things that we've been dealing with, is this thing of cyber perfection.

0:11:03
So keep in mind—absolute security is absolutely impossible. So design systems to be resilient and tolerate cyber failure and yet enable mission and business and things to keep on working, despite the fact that an event has occurred. Build and deliver cloud-native applications to take full advantage of these advanced cloud features. Fully leverage things like elastic computing and software defined networking. The objective here is let's make it a shell game. If they can't find you, they can't attack you. And we know how to do this. We know how to hide ourselves. And then apply really some advanced techniques—deterministic code development and polymorphic code development techniques, harden applications, and turn us into a polymorphic attack surface, instead of the adversary being a polymorphic attacker on us. All of these things are real today, some albeit more mature than others across the board—I

don't deny that. But just as in the Apollo program, it was the ingenuity of the people themselves and a focused action that we could bring these together in a way that actually created a much better outcome across the board.

0:12:02
So I'm running slightly over time, so I'm going to apologize for that. But I think what I want to make sure you understand is we don't want to oversimplify the problem. This is a really difficult thing to do. And given the complexities [0:12:16] surround it—it's just—there's more to this than what I mentioned. And so other things I'd like you to keep in mind as we look at this and drive to a cyber moonshot is around providing things like incentives to harden data and systems that actually outweigh the cost of inaction. And today, I don't think we have those in place. Our current approach to cyber I think is actually broken. We have an every man for themself approach to deal with this thing, and that just exacerbates the situation. And in a world of the weakest link, we are held hostage by those who don't have sufficient resources in order to make themselves a really strong cyber posture. Talent remains a huge issue across the board, and we have to solve that problem. But by the way, I will tell you the every man for himself approach exacerbates that problem and makes it difficult to—and creates just competition for limited resources. So think common and shared services.

0:13:06
And then we've got to find ways to share data. You heard that also. We must share data. I think we need to look at cyber threat data as a common good for the common people, and use it, and find ways to make it immediately available for everybody to take advantage of and do. So of course there are many other challenges and things like that, but what this is all about is bringing us together to achieve a common goal for the good of all. Because it's going to take all of us to land the cyber moonshot. So anyhow, I want to close by saying, keep in mind that it's not that we're not

doing great things. It's just that I believe—we believe—that we're lacking coherent purpose and vision, and a call to action to do this. And that's the objective of the cyber moonshot. So when you leave here today, I hope you'll join us for the call for the moonshot. I hope that you'll provide leadership and commitment that we need to achieve it, and establish a relentless focus on the goal and understand what it means for your organization across the board. And then go tell others about it.

0:14:01
We have papers that go into detail on what I just talked about, out front. So please pick up several copies and take it to your friends. We'll also make sure they're available to you digitally. And as I didn't ever change my slides when I was going through this thing and talking across the board, we'd like to hear from all of you and understand what it's going to take to ignite this effort across the board. And thank you so much, and I appreciate your time.

[applause]

[End of recording]